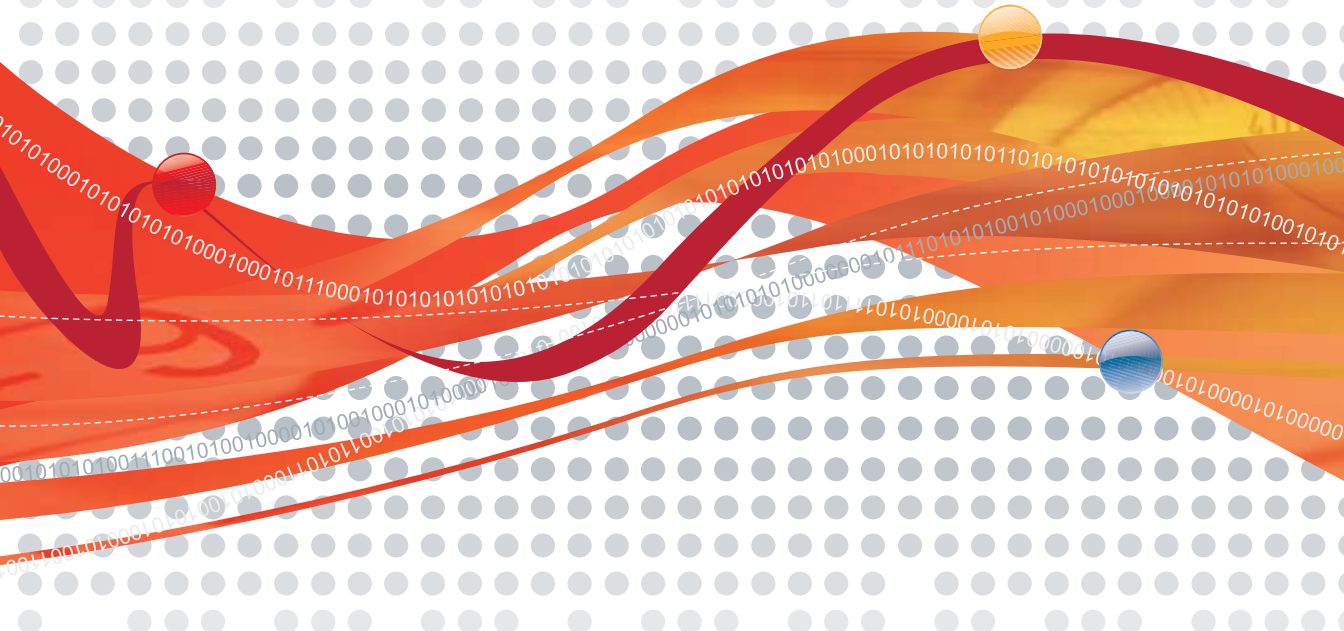
TREND MICRO

InterScan™ Web Security Virtual Appliance 5

Antivirus and Content Security at the Web Gateway

Installation Guide



Web Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Trend Micro, the Trend Micro t-ball logo, LeakProof are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 1998-2009 Trend Micro Incorporated. All rights reserved.

Release Date: June 2009

Protected by U.S. Patent No. 5,951,698

The Installation Guide for Trend Micro™ InterScan™ Web Security Virtual Appliance is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Audience x
IWSVA Documentation xi
Document Conventions xii
About Trend Micro 1-xiii

Chapter 1: Pre-installation Planning

Server Requirements 1-2
- Operating System 1-2
- Hardware Requirements 1-2
- Web Browser 1-3
- Other Requirements 1-4

Information Needed to Install IWSVA 1-5
- Fresh Installation 1-5
- Migration 1-5
- Type of Proxy Configuration 1-6
- Control Manager Server Information 1-6
- Database Type and Location 1-6
- SNMP Notifications 1-6
- Web Console Password 1-6
- Command Line Access 1-7
- Proxy for Internet Updates 1-7
- Activation Codes 1-7

Planning Network Traffic Protection 1-7
- Transparent Bridge Mode 1-8
- Forward Proxy Mode 1-8
- ICAP Mode 1-8
- Reverse Proxy Mode 1-9

Chapter 2: Deployment Primer

Identifying Your Server Placement 2-2
Two Firewalls with DMZ 2-2
One Firewall with No DMZ 2-3
Planning HTTP and FTP Service Flows 2-4
Planning the HTTP Flow 2-5
HTTPs Decryption 2-7
Planning FTP Flows 2-7
FTP Proxy in Stand-alone Mode 2-7
FTP Proxy in Dependent Mode 2-9
Deploying in Forward Proxy Mode 2-10
Overview of Forward Proxy Mode 2-10
Reconfiguring Client Settings 2-11
Using a Layer 4 Switch 2-12
Using a WCCP-enabled Switch or Router 2-14
Planning the HTTP Flow Using Forward Proxy Mode 2-15
HTTP Proxy in Standalone Mode 2-15
HTTP Proxy in Simple Transparency Mode 2-16
HTTP Proxy in Dependent Mode (Proxy Ahead) 2-17
HTTP Proxy in Dependent Mode (Proxy Behind) 2-19
HTTP Double Proxy in Dependent Mode 2-21
HTTP Proxy in WCCP Mode (Single and Multiple IWSVA Servers) 2-22
Deploying in ICAP Mode 2-23
Overview of ICAP Mode 2-23
Planning the HTTP Flow Using ICAP Mode 2-25
HTTP Proxy in ICAP Mode (Single and Multiple IWSVA Servers) 2-25
IWSVA ICAP Mode with Multiple Servers 2-27
Deploying in Reverse Proxy Mode 2-29
Overview of Reverse Proxy Mode 2-29
Planning the HTTP Flow Using Reverse Proxy Mode 2-30
HTTP Reverse Proxy in Dependent Mode 2-30
Deploying in Transparent Bridge Mode 2-32
Overview of Transparent Bridge Mode 2-32
Planning the HTTP Flow Using Transparent Bridge Mode 2-33

Chapter 3: Installing InterScan Web Security Virtual Appliance

Operating System Requirements 3-2
Component Installation 3-2
Obtaining IWSVA 3-3
Installing IWSVA 3-4
Choosing a Deployment Mode for the Installation 3-11
Installing for Transparent Bridge Mode 3-11
Installing for Forward Proxy Mode 3-13
Installing for ICAP Mode 3-18
Installing for Reverse Proxy Mode 3-21
Logging Into IWSVA for the First Time 3-23
Post-Installation Notes 3-24

Chapter 4: Migrating to IWSVA

About Migration 4-2
Important Notes 4-2
Information Not Migrated 4-3
Overview of the Migration Process 4-4
Migrating from IWSS 3.1 Linux/Windows or IWSA 3.1 SP1 to IWSVA 5.0 4-5
Migrating from IWSVA 3.1 to IWSVA 5.0 4-5
Migrating from IWSVA 5.0 to another IWSVA 5.0 4-6

Appendix A: Deployment Integration

IWSVA in a Distributed Environment A-2
Connection Requirements and Properties A-2
Throughput and Availability Requirements A-3
Integration with LDAP A-4
Support Referral Chasing for Multiple LDAP Servers A-4
LDAP Authentication in Transparent Mode A-6
Damage Cleanup Services (DCS) Integration A-7
Using SSL with Damage Cleanup Services (DCS) A-9
Integration with a Cisco Router using WCCP A-10
Configuring the Cisco device and IWSVA for WCCP A-11
Configuring WCCP Assignment Method A-13
Configuring IWSVA for a WCCP Service Group A-13
Load Balancing for WCCP Communication A-13

Configuring IWSVA to use the Dynamic Service Group A-14
Configuring IWSVA to use the Well-Know Service Group A-15
Configuration 1: Firewall only between WCCP Router and Internet . A-16
Configuration 2: Firewall on Client Machine A-17
Configuration 3: Stateful Firewall Between Client and IWSVA A-17
Controlling WCCP Logging A-18
Sample PIX Firewall Configuration A-18
Protecting an HTTP or FTP Server using Reverse Proxy A-19
Integration with an ICAP Device A-20
Setting up an ICAP 1.0-compliant Cache Server A-20
Setting up ICAP for NetCache Appliances A-21
Setting up ICAP for Blue Coat Port 80 Security Appliance A-23
Setting up ICAP for Cisco CE ICAP Servers A-26
Configuring Virus-scanning Server Clusters A-27
Deleting a Cluster Configuration or Entry A-28
Enabling “X-Virus-ID” and “X-Infection-Found” Headers A-28
Configuring the Local Squid Proxy A-29

Appendix B: Tuning and Troubleshooting

IWSVA Performance Tuning B-2
URL Filtering B-2
LDAP Performance Tuning B-2
LDAP Internal Caches B-3
Disable Verbose Logging When LDAP is Enabled B-4
LDAP Authentication in Transparent Mode B-4
Troubleshooting B-6
Troubleshooting Tips B-6
Before Contacting Technical Support B-6
Installation Problems B-6
General Feature Problems B-7

Appendix C: Additional IWSVA Testing

EICAR Test File C-1
Testing Web Reputation C-2
Testing Upload Scanning C-2
Testing HTTPS Decryption Scanning C-3

Testing FTP Scanning C-5
Testing URL Monitoring C-7
Testing Download Scanning C-8
Testing URL Filtering C-9
Testing Spyware Scanning C-10
Testing PhishTrap C-11
Testing Java Applet and ActiveX Scanning C-12
Testing IntelliTunnel Security C-13

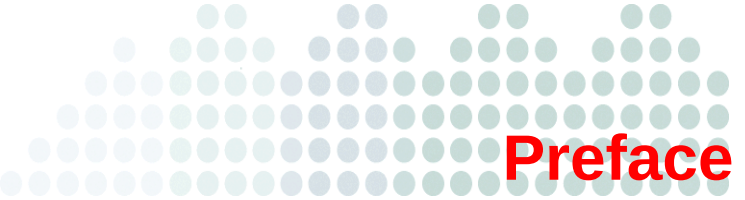
Appendix D: Maintenance and Technical Support

Product Maintenance D-2
Maintenance Agreement D-2
Renewing Your Maintenance Agreement D-3
Contacting Technical Support D-4
TrendLabs D-4
Knowledge Base D-5
Known Issues D-5
Sending Suspicious Code to Trend Micro D-6
Security Information Center D-7

Appendix E: Creating a New Virtual Machine Under VMware ESX for IWSVA

Creating a New Virtual Machine E-2

Index



Preface

Welcome to the *Trend Micro™ InterScan Web Security Virtual Appliance 5.0 Installation Guide*. This guide helps you to get “up and running” by introducing IWSVA, assisting with deployment, installation, migration (if necessary), initial configuration, troubleshooting, performance tuning, and main post-installation configuration tasks. It also includes instructions on testing your installation using a harmless test virus, troubleshooting, and accessing support.

This preface describes the following topics:

- Audience
- IWSVA Documentation
- Document Conventions

Audience

The IWSVA documentation is written for IT managers and system administrators working in enterprise environments. The documentation assumes that the reader has in-depth knowledge of networks schemas, including details related to the following:

- HTTP and FTP protocols
- Database configuration
- VMware ESX administration experience when installing on VMware ESX

The documentation does not assume the reader has any knowledge of antivirus or Web security technology.

How to Use this Guide

This guide contains the information you need to understand and use IWSVA.

If you are an advanced user, you might want to go directly to Chapter 3, *Installing InterScan Web Security Virtual Appliance* and Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA*.

Chapter 1, *Pre-installation Planning*	This chapter describes the tasks you need to do before installing IWSVA. This includes planning for network traffic and HTTP and FTP service flows and ensuring that your server meets specific requirements.
Chapter 2, *Deployment Primer*	This chapter provides an overview of the different topologies that IWSVA can be installed in and helps you plan your server placement and network protection with HTTP and FTP service flows.
Chapter 3, *Installing InterScan Web Security Virtual Appliance*	This chapter describes how to obtain either a trial or production version of IWSVA and how to install the application.
Chapter 4, *Migrating to IWSVA*	This chapter describes the different migration scenarios and how to complete a migration to IWSVA.

Appendix A, *Deployment Integration*	This appendix describes deployment scenarios for IWSVA, involving several technologies such as LDAP, Damage Cleanup Services (DCS), Cisco routers using WCCP, ICAP, Transparent Bridge, and Local Squid Proxy.
Appendix B, *Tuning and Troubleshooting*	This appendix describes performance tuning involving URL filtering and LDAP performance. Also, this appendix provides general troubleshooting tips and possible installation and feature issues.
Appendix C, *Additional IWSVA Testing*	This appendix describes the testing of various IWSVA features that involve scanning, blocking, and filtering.
Appendix D, *Maintenance and Technical Support*	This appendix describes the maintenance agreement and the aspects of the Trend Micro Technical Support Center.
Appendix E, *Creating a New Virtual Machine Under VMware ESX for IWSVA*	This appendix describes how to create a new virtual machine for IWSVA.

IWSVA Documentation

In addition to the *Trend Micro™ InterScan Web Security Virtual Appliance 5.0 Installation Guide*, the documentation set includes the following:

- **Administrator's Guide**—this guide provides detailed information about all IWSVA configuration options. Topics include how to update your software to keep protection current against the latest risks, how to configure and use policies to support your security objectives, and using logs and reports.
- **Readme file**—the Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

  The latest versions of the Installation Guide, Administrator's Guide, and readme file are available in electronic form at:

http://www.trendmicro.com/download/

CD ISO creation document—Entitled, *How to Use the Trend Micro IWSVA ISO File*, this document describes how to create a bootable installation CD from an ISO file.

Online Help—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon.
The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the IWSVA management console.

- **Knowledge Base**—the Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://esupport.trendmicro.com/support`

- **TrendEdge**—a program for Trend Micro employees, partners, and other interested parties that provides information on unsupported, innovative techniques, tools, and best practices for Trend Micro products. The TrendEdge database contains numerous documents covering a wide range of topics.

  `http://trendedge.trendmicro.com`

Document Conventions

To help you locate and interpret information easily, the InterScan Web Security Virtual Appliance documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway-gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

`http://www.trendmicro.com`

Chapter 1

Pre-installation Planning

This chapter describes the following:

- Server Requirements
- Information Needed to Install IWSVA
- Planning Network Traffic Protection

Server Requirements

Operating System

A purpose-built, hardened, and performance-tuned 64-bit operating system is included with InterScan Web Security Virtual Appliance (IWSVA).

Hardware Requirements

Minimum Requirements:

- Single 2.0 GHz Intel ™ Core2Duo™ 64-bit processor supporting Intel™ VT™ or equivalent
- 2GB RAM
- 12GB of disk space. IWSVA automatically partitions the detected disk space as required
- Monitor that supports 1024 x 768 resolution with 256 colors or higher

Recommended Requirements:

- Dual 2.8 GHz Intel ™ Core2Duo™ 64-bit processor or equivalent for up to 4000 users
- Dual 3.16 GHz Intel ™ QuadCore™ 64-bit processor or equivalent for up to 9500 users
- 4GB RAM is recommended to support up to 4000 users
- 8GB RAM is recommended to support up to 9500 users
- 300GB of disk space or more for log intensive environments. IWSVA automatically partitions the detected disk space as per recommended Linux practices

Server Platform Compatibility

IWSVA should install and operate without issues on many brands of “off-the-shelf” server platforms. However, Trend Micro cannot guarantee 100% compatibility with all brands and models of server platforms.

To obtain a list of Trend Micro certified servers that are compatible with IWSVA, access the following URL:

`http://www.trendmicro.com/go/certified`

To obtain a general list of available platforms that should operate with IWSVA, access the following URL:

`http://wiki.centos.org/HardwareList`

Trend Micro cannot guarantee full compatibility with the hardware components from this general list.

Web Browser

To access the HTTP-based Web console, use any of the browsers in Table 1-1.

TABLE 1-1. Supported Web Browsers for Web Console Access

BROWSER	WINDOWS		UNIX
	XP SP2	VISTA (64-BIT)	RH 4.0 AS
IE 6.0	✓		
IE 7.0	✓	✓	
IE 8.0	✓	✓	
Firefox 3.0	✓	✓	✓

To access the Internet through IWSVA, use any of the browsers in Table 1-2.

TABLE 1-2. Supported Web Browsers for Internet Access

BROWSER	WINDOWS		UNIX	MAC
	XP SP2	VISTA (64-BIT)	RH 4.0 AS	OS X
IE 6.0	✓			
IE 7.0	✓	✓		
IE 8.0	✓	✓		
Firefox 3.0	✓	✓	✓	

TABLE 1-2. Supported Web Browsers for Internet Access (Continued)

BROWSER	WINDOWS		UNIX	MAC
Safari 3.0				✓

Other Requirements

- **Database requirements:**
  - PostgreSQL v7.4.16 (included)
  - When using multiple IWSVA servers in a server farm configuration, Trend Micro recommends that you use separate server (possibly clustered) for PostgreSQL
  - 1.7GB of disk space for every three million HTTP requests per day in order to maintain log files (calculation based on access logging enabled)
  - 256MB of RAM (based on access logging enabled, else 64MB)
- **Internet Content Adaptation Protocol (ICAP):**
  - NetApp™ NetCache™ release 6.0.1
  - Blue Coat Systems™ SGOS v5 (latest version)
  - Cisco ICAP servers: CE version 5.3
  - Any cache server that is ICAP 1.0 compliant
- **Directory Servers:**

  To configure policies based on Lightweight Directory Access Protocol (LDAP) users and groups, IWSVA can integrate with the following LDAP directories:
  - Microsoft Active Directory 2000 and 2003
  - Linux OpenLDAP Directory 2.2.16 or 2.3.39
  - Sun™ Java System Directory Server 5.2 (formerly Sun™ ONE Directory Server)
- **Transparent Bridge:**
  - Two network cards are required for IWSVA to support this configuration.
- **Web Cache Content Protocol (WCCP):**

  Trend Micro recommends using the following Cisco IOS versions when configuring WCCP with IWSVA:

  - 12.2(0) to 12.2(22). Avoid using releases 23 and above within the 12.2 family
  - 12.3(10) and above. Avoid using releases 0-9 in the 12.3 family
  - IOS 12.4(15)T3 or later should be used
- **Other requirements:**
- For proxy deployment modes, network clients must be able to access the HTTP port of the IWSVA server that is selected during the install.
- IWSVA server and clients must be able to communicate with each other over the corporate network.

Information Needed to Install IWSVA

You can either purchase or download a 30-day trial version of IWSVA. The 30-day trial version provides all the functionality of IWSVA.

The IWSVA setup program prompts you for required information, depending on the options chosen during installation.

Fresh Installation

IWSVA only supports fresh installations — upgrading an existing IWSS or IWSA installation is not supported. The fresh installation process formats your existing system to install IWSVA. (see Installing IWSVA on page 3-4).

Migration

IWSVA supports existing configuration and policy data migration from the following Trend Micro Products:

- InterScan Web Security Suite 3.1 Linux
- InterScan Web Security Suite 3.1 Windows
- InterScan Web Security Appliance 3.1 Service Pack 1
- InterScan Web Security Virtual Appliance 3.1
- InterScan Web Security Virtual Appliance 5.0 (same language version)

For more information about migration, see Chapter 4, Migrating to IWSVA.

Type of Proxy Configuration

IWSVA supports multiple deployment modes.

- Forward proxy where clients directly connect to IWSVA.
- Upstream proxy to another existing internal proxy server
- ICAP Server to an existing ICAP 1.0 compliant cache controller
- WCCP client to a configured WCCP-enabled router of firewall
- Transparent Bridge Mode
- Reverse proxy to protect a Web server

The deployment is configured during the IWSVA installation and it can be changed using the management interface. The dependency for the Transparent Bridge Mode deployment is the minimum of two network cards. See Planning the HTTP Flow on page 2-5 and Planning FTP Flows on page 2-7.

Control Manager Server Information

Control Manager registration is performed through the IWSVA Web UI after the IWSVA installation is complete.

Database Type and Location

IWSVA uses the PostgreSQL database for report logs, policies, rules, and configuration settings. A local PostgreSQL installation is performed during IWSVA installation.

SNMP Notifications

If you plan to use SNMP notifications, the IWSVA setup program installs the appropriate SNMP libraries.

Web Console Password

Access to the IWSVA Web console is controlled through a username and password that are set during installation.

Command Line Access

IWSVA provides a Command Line Interface (CLI) to allow configuration of the appliance using an industry standard CLI syntax. The CLI offers additional commands and functionality to manage, troubleshoot, and maintain the IWSVA. The CLI can be accessed using a local console keyboard and monitor or remotely through SSHv2.

Proxy for Internet Updates

If you have a proxy host between IWSVA and the Internet, you must configure the IWSVA's proxy settings in order to receive updates from Trend Micro. From the menu, choose **Updates > Connection Settings** to configure the upstream proxy setting. See the Administrator's Guide for completed details.

Activation Codes

Activating the three IWSVA modules (core program, URL Filtering, and Applet and ActiveX Scanning) requires three separate activation codes. IWSVA comes with registration keys for the modules purchased. During product registration, the Registration Keys are exchanged for Activation Codes that "unlock" the program. You can register the installation and exchange registration keys for activation codes from a link in the setup program. Alternatively, you can register and obtain activation codes before installing by visiting Trend Micro's online registration Web site at:

`http://olr.trendmicro.com`

Planning Network Traffic Protection

IWSVA can be deployed in different modes to help secure your network (see Choosing a Deployment Mode for the Installation on page 3-11). IWSVA supports the following deployment topologies:

- Transparent Bridge Mode
- Forward Proxy Mode
- ICAP Mode
- Reverse Proxy Mode

Transparent Bridge Mode

IWSVA acts as a bridge between network devices such as routers and switches. IWSVA scans passing HTTP and FTP traffic without the need to modify browser or network settings. This is the easiest deployment mode with traffic scanned in both directions.

The additional dependency for this deployment mode is two network cards. Trend Micro recommend that in this deployment mode the following network cards be used to ensure maximum compatibility:

- Broadcom NetXtreme Series
- Intel Pro/1000 PT Dual Port Server Adapter
- Intel Pro/1000 MF Dual Port Fiber

For further details on Transparent Bridge Mode, see Deploying in Transparent Bridge Mode on page 2-32.

Forward Proxy Mode

IWSVA acts as an upstream proxy for network clients. Client browser settings must be configured to redirect traffic to IWSVA. IWSVA scans HTTP and FTP traffic and there is no separate need for another dedicated proxy server. Content is scanned in both the inbound and outbound directions.

Forward Proxy Mode also provides the following additional capabilities:

- Forward all traffic to a further upstream proxy server
- Integration with an L4 switch for load balancing and simple transparency
- Integration with a WCCP enabled switch or firewall for load balancing and simple transparency

For further details on Forward Proxy mode, see Deploying in Forward Proxy Mode on page 2-10.

ICAP Mode

IWSVA acts as an ICAP proxy and accepts ICAP connections from an ICAP v1.0 compliant cache server. Cache servers can help reduce the overall bandwidth

requirements and reduce latency by serving cached content locally. IWSVA scans and secures all content returned to the cache server and to the clients.

For further details on ICAP mode, see Deploying in ICAP Mode on page 2-23.

Reverse Proxy Mode

IWSVA is deployed in front of a Web server. IWSVA scans HTTP and FTP content from the clients that are uploaded to a web server as well as content that is downloaded from the Web server to the clients and helps secure the Web server.

For further details on the Reverse Proxy Mode, see Deploying in Reverse Proxy Mode on page 2-29.

Chapter 2

Deployment Primer

This chapter describes the following:

- Identifying Your Server Placement
- Planning HTTP and FTP Service Flows
- Deploying in Forward Proxy Mode
- Deploying in ICAP Mode
- Deploying in Reverse Proxy Mode
- Deploying in Transparent Bridge Mode

Identifying Your Server Placement

Before installing IWSVA, you will need to review the IWSVA deployment modes and decide how best to install IWSVA into your network environment to meet your needs. This involves identifying where to place the IWSVA server in the network and identifying the best deployment mode for your network.

Today's enterprise network topologies typically fall into one of two categories:

- Two firewalls with a Demilitarized Zone (DMZ)
- One firewall without a DMZ.

The ideal location for the IWSVA server depends upon the topology in use.

Two Firewalls with DMZ

Given today's security concerns, many organizations have implemented a topology consisting of two firewalls (one external and one internal). These firewalls divide the network into two main areas:

- **The DMZ**—The DMZ is located between the external and internal firewalls. Hosts that reside in this area can accept connections from servers that are external to the organization's network. The configuration of the external firewall lets packets from external computers only reach servers inside the DMZ.

- **Corporate LAN**—These segments are located behind the internal firewall. The configuration of the internal firewall passes traffic to machines on the corporate LAN only when the traffic originates from computers inside the DMZ.

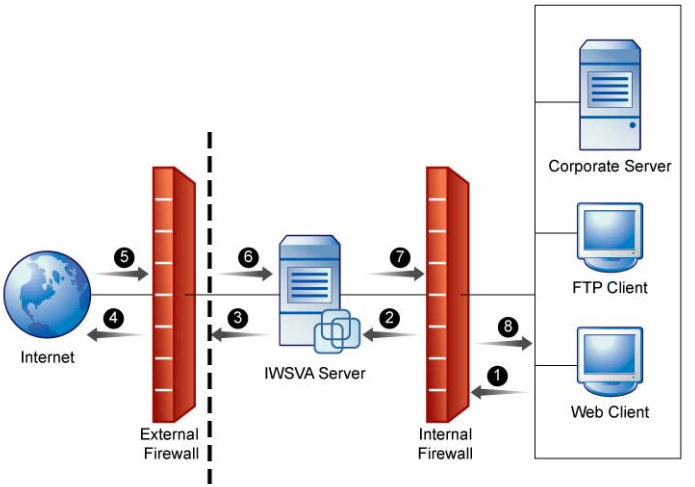


FIGURE 2-1 Two Firewalls with DMZ

This topology requires that all data inbound from the external servers (such as those on the Internet) first pass through a server in the DMZ. It also requires that certain types of data (for example HTTP and FTP packets), outbound from internal segments, pass through a server in the DMZ. This forces the use of proxies such as IWSVA.

One Firewall with No DMZ

Some organizations have a firewall, but no DMZ. When using the “no DMZ” topology place the IWSVA server behind the firewall.

- Because the IWSVA server is not isolated from the corporate LAN, there is one less hop between external machines and machines on the corporate LAN. As shown in the diagram, this results in two less steps for processing a request, one outbound and one inbound.

- The firewall configuration allows connections to machines on the corporate LAN. For security, the firewall must limit the types of data that can reach machines on the LAN. For example, the firewall might allow HTTP data from the Internet to reach only the IWSVA server.

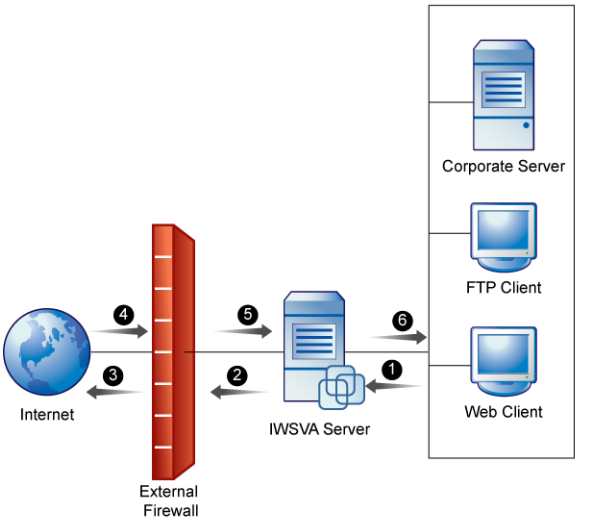


FIGURE 2-2 One Firewall with DMZ

Planning HTTP and FTP Service Flows

Network Traffic

To enforce the network traffic protection using IWSVA, an additional solution (hardware, software or configuration) must be introduced that redirects the HTTP and/or FTP traffic to IWSVA. This solution includes the following:

- Reconfiguring client settings
- Using a Layer 4 switch
- Using an ICAP-enabled proxy
- Using WCCP
- Using a local Squid 3.0 cache

See Appendix A, Deployment Integration starting on page A-1 for complete details.

HTTP and FTP Service Flows

Each HTTP and FTP configuration has implications for configuring IWSVA, configuring the network, and for network security.

Create a flow plan for the HTTP and FTP services by doing the following:

- Understand each IWSVA service's purpose and function
- Determine each service's valid data sources. For example, does the HTTP service receive requests directly from the HTTP browsers, or indirectly through an ICAP proxy device?
- Determine which ports to use for the service. For instance, by default, the HTTP proxy service uses port 8080, and the FTP service uses port 21. However, if another application or service is using port 8080, the administrator must configure the HTTP proxy service to use a different port.
- Determine each service's valid data destinations. For example, does the HTTP proxy service send validated requests directly to the Web site? Or, does the HTTP proxy service send the validated request to an upstream HTTP proxy?
- Add in any service-specific considerations. For instance, the HTTP service flow might include an ICAP device, but the FTP service flow does not.

Using the information gathered above, administrators can determine which one of the possible flows to use for the installation.

Planning the HTTP Flow

The first step when planning HTTP flow for IWSVA is choosing the way HTTP traffic is processed by IWSVA (the deployment mode):

- HTTP Proxy
- ICAP device
- WCCP device
- Transparent Bridge
- Simple Transparency
- Reverse Proxy

The flow involving an ICAP or WCCP device is very different from those that do not involve ICAP or WCCP devices.

There are seven possible flows:

Transparent Bridge Settings

- **Transparent Bridge mode** — Use the transparent bridge mode when clients' computers are not configured to use the IWSVA server as their proxy, but still need to connect to the Internet through IWSVA.

Forward Proxy Settings:

- **Standalone mode** — Use this flow when ICAP devices are not being used with IWSVA, and IWSVA connects directly to the Internet.
- **Dependent mode** — Use this flow when ICAP devices are not being used with IWSVA, and IWSVA cannot connect directly to the Internet, but must instead connect through another HTTP proxy. This is can be accomplished in one of the following ways:
  - Proxy-ahead mode
  - Proxy-behind mode (not recommended)
  - Double-proxy mode
- **Forward Proxy with Transparency —** Use this mode when using an L4 (Load Balancing) switch.
- **WCCP** — Use the WCCP protocol in conjunction with WCCP enabled devices with IWSVA

Reverse Proxy Settings:

- **Reverse proxy mode —** Use this flow to protect a Web server with a proxy server by placing the HTTP proxy between the Internet and the Web server. (Used by ISPs and ASPs to protect the upload traffic against viruses and by organizations with complex Web sites that need a centralized point of access control.)

ICAP Proxy Settings:

- **ICAP protocol mode** — Use the ICAP protocol flow to use ICAP devices with IWSVA

Each configuration has implications for configuring IWSVA, configuring the network, and for network security.

HTTPs Decryption

IWSVA closes the HTTPs security loophole by decrypting and inspecting encrypted content. You can define policies to decrypt HTTPs traffic from selected Web categories. While decrypted, data is treated the same way as HTTP traffic to which URL filtering and scanning rules can be applied.

IWSVA supports HTTPs decryption and scanning in the following modes:

- Transparent bridge
- WCCP
- Forward proxy

Planning FTP Flows

There are two possible FTP flows: stand-alone and dependent. They are similar to the stand-alone and dependent-mode flows for HTTP service. Each requires a different configuration and has its own implications including:

- **Stand-alone**—the IWSVA server acts as an FTP proxy server between the requesting client and the remote site, brokering all transactions
- **Dependent**—IWSVA works in conjunction with another FTP proxy server within a LAN

FTP Proxy in Stand-alone Mode

To scan all FTP traffic in and out of the LAN, set up the FTP scanning module so that it “brokers” all such connections. In this case, clients FTP to the IWSVA server, supply the logon credentials to the target site, and then allow the IWSVA FTP server to make the connection. The remote site transfers the files to IWSVA FTP. Before delivering the files to the requesting clients, the IWSVA FTP server scans the files for viruses and other security risks.

The implications for the FTP stand-alone flow are:

- IWSVA must have access to the target FTP servers
- There is one less step in the flow, compared to the FTP proxy mode

To configure FTP clients to use this flow:

- Set the IWSVA server as a FTP proxy

- Set the user name to be `username@targetftp-server`, instead of the normal username

Note: IWSVA FTP works with most firewalls, usually requiring only a modification to the firewall to open a port for the FTP proxy.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSVA FTP service.
2. The IWSVA FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSVA FTP service attempts to connect to the appropriate FTP server on the Internet. If the connection succeeds, the IWSVA FTP service sends the request to the target FTP server.
3. The FTP server on the Internet responds to the request, ideally with the requested file.
4. The IWSVA FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

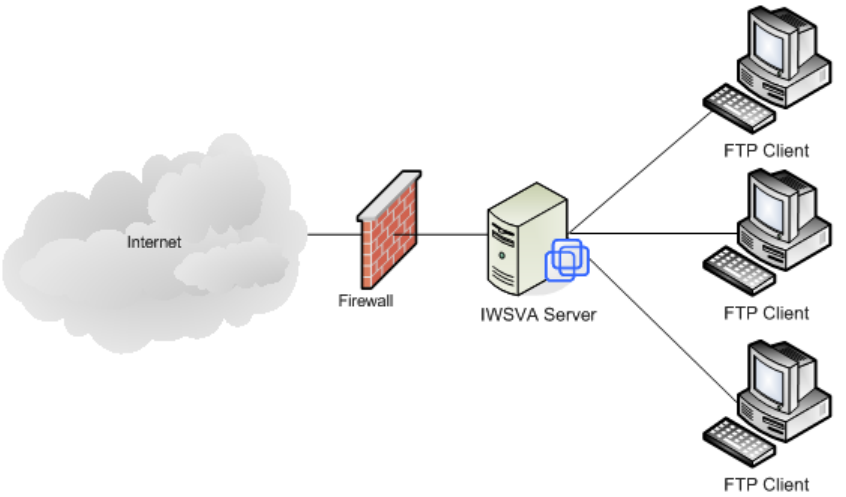


FIGURE 2-3 FTP Proxy in Standalone Mode

FTP Proxy in Dependent Mode

You can also install IWSVA FTP on a dedicated machine between an upstream proxy and the requesting clients. Using this setup adds other FTP features (for example, access blocking, logging, and filtering) to supplement the existing FTP proxy.

IWSVA's FTP-proxy mode, shown in Figure 2-4, is analogous to the dependent-mode flow of the HTTP service. Because it carries a performance penalty of an extra hop and extra processing by the other FTP proxy server, only use this mode if your organization does not allow the IWSVA Server to access the Internet directly.

If the other FTP proxy server uses a store-and-forward technique, the performance penalty is more noticeable on large files because the other FTP proxy first downloads the file and passes it on to the IWSVA FTP service. Additionally, the other FTP proxy must have sufficient free disk space to hold all transfers in progress.

Unlike the HTTP dependent-mode service, which has the possible benefit of cached requests, most FTP proxy servers do not cache requests.

FTP Dependent Mode also protects FTP servers from upload and download threats.

FTP requests follow this sequence:

1. The FTP client sends a request to the IWSVA FTP service.
2. The IWSVA FTP service validates the request (for example, the file type is not blocked). If the request is valid, the IWSVA FTP service relays it to the other FTP proxy or the FTP server being protected by IWSVA.
3. The FTP server on the Internet responds to the request, ideally with the requested file.

4. The IWSVA FTP service scans the returned data for unwanted content. If it finds any unwanted content, it returns an appropriate message to the FTP client. Otherwise, it returns the requested data to the FTP client.

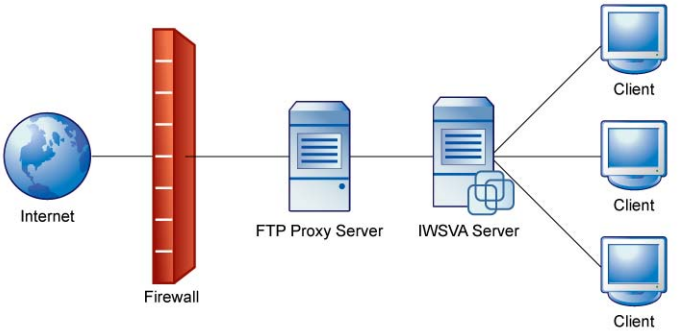


FIGURE 2-4 FTP Proxy in Dependent Mode

Deploying in Forward Proxy Mode

Overview of Forward Proxy Mode

There are two kinds of Forward Proxy: non-transparent and transparent. Transparent proxy can be achieved by a Layer 4 switch (Simple Transparency) or a WCCP-enabled switch (WCCP mode).

IWSVA configured in forward proxy mode provides the following configuration options to enable client protection:

- Reconfiguring Client Settings
- Using a Layer 4 Switch
- Using a WCCP-enabled Switch or Router

Additionally, when IWSVA is configured in this mode, all traffic can be configured to be sent to an additional upstream proxy server if applicable.

The configuration options are explored in the table below to provide information to help decide which deployment configuration to use.

During the IWSVA installation, select to install IWSVA in Forward Proxy Mode to support this configuration.

Reconfiguring Client Settings

HTTP clients (browser or proxy servers) can be configured to contact IWSVA as a proxy. This configuration change ensures that the client's Web traffic is forwarded to IWSVA. The HTTP scanning service must be enabled in the HTTP Proxy mode to process this traffic.

FTP clients must contact IWSVA instead of the destination server, and use a modified handshake to supply the FTP server address. The FTP scanning module must be installed and configured in standalone mode to process this traffic.

TABLE 2-1. Reconfiguring the Client Settings

ADVANTAGE	LIMITATION
No additional hardware required	Administrator have to control settings for all computers. (Guest computers can have difficulties.)

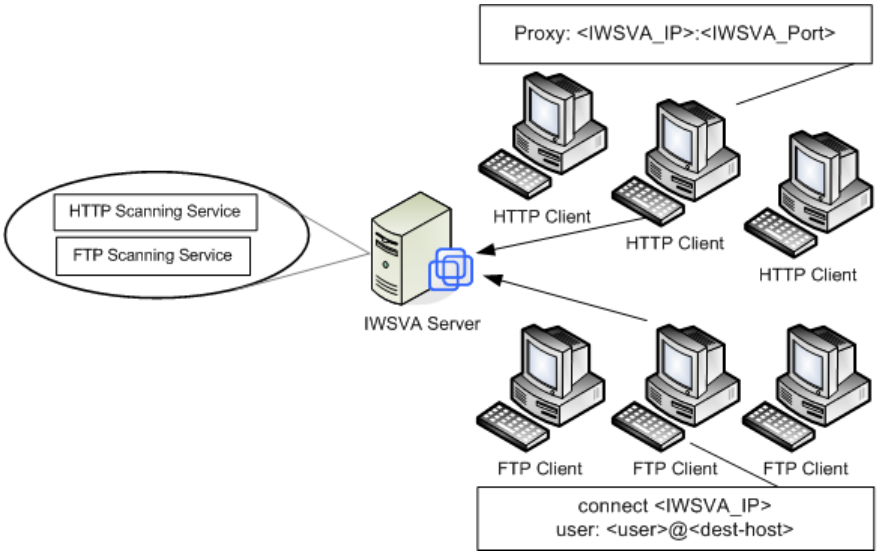


FIGURE 2-5 Reconfiguring the Client Settings

Using a Layer 4 Switch

Transparency is the functionality whereby client users do not need to change their Internet connection's proxy settings to work in conjunction with IWSVA. Transparency is accomplished with a Layer 4 switch that redirects HTTP packets to a proxy server, which then forwards the packets to the requested server.

IWSVA supports "simple" type transparency. Simple transparency is supported by most Layer 4 switches. While it is compatible with a wide variety of network hardware from different manufacturers, configuring simple transparency does impose several limitations:

- When using simple transparency, the User Identification method to define policies is limited to IP address and/or host name; configuring policies based on LDAP is not possible.
- FTP over HTTP is not available; thus, links to ftp:// URLs might not work if your firewall settings do not allow FTP connections. Alternatively, links to ftp:// URLs might work, but the files will not be scanned.

- Simple transparency is not compatible with some older Web browsers when their HTTP requests do not include information about the host.
- HTTP requests for servers that use a port other than the HTTP default port 80 are redirected to IWSVA. This means SSL (HTTPS) requests are typically fulfilled, but the content is not scanned.
- Do not use any source NAT (IP masquerade) downstream of IWSVA, because IWSVA needs to know the IP address of the client to clean.
- A DNS server is needed for DCS to resolve the client machine name from its IP address in order to perform a cleanup.

A Layer 4 switch can be used to redirect HTTP traffic to IWSVA. The HTTP Scanning Service must be enabled in the HTTP Proxy mode.

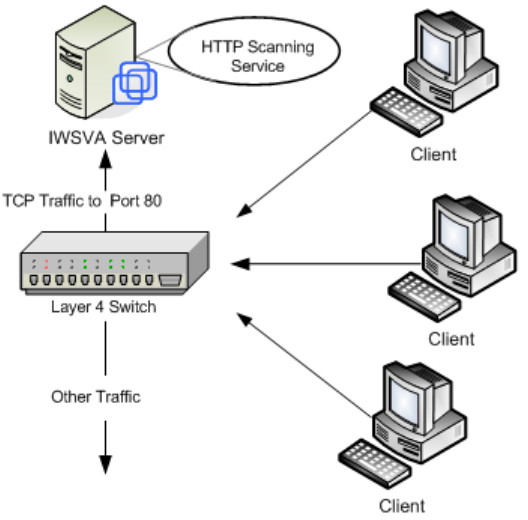


FIGURE 2-6 Using a Layer 4 Switch

During the installation, ensure that the check box that enables transparency to support this deployment mode is checked.

TABLE 2-2. Using a Layer 4 Switch

ADVANTAGES	LIMITATIONS
Transparent to clients	Traffic interception must be port-based (not protocol-based) for one port. If the non-standard port is used for HTTP, it bypasses the switch.
Simple to establish	The switch-based redirection cannot be used for the FTP traffic.
	No LDAP support

Using a WCCP-enabled Switch or Router

IWSVA supports WCCP v2.0 and forwarding methods based on GRE and L2 (layer 2).

When using WCCP transparency, FTP downloads are also scanned. With the ability to support WCCP v2.0, IWSVA is able to participate in a cluster of IWSVA devices to provide a load balancing WCCP Web security platform.

Advantages of using WCCP:

- Transparency for client side
- Scalable

Limitations of using WCCP:

- Cisco proprietary

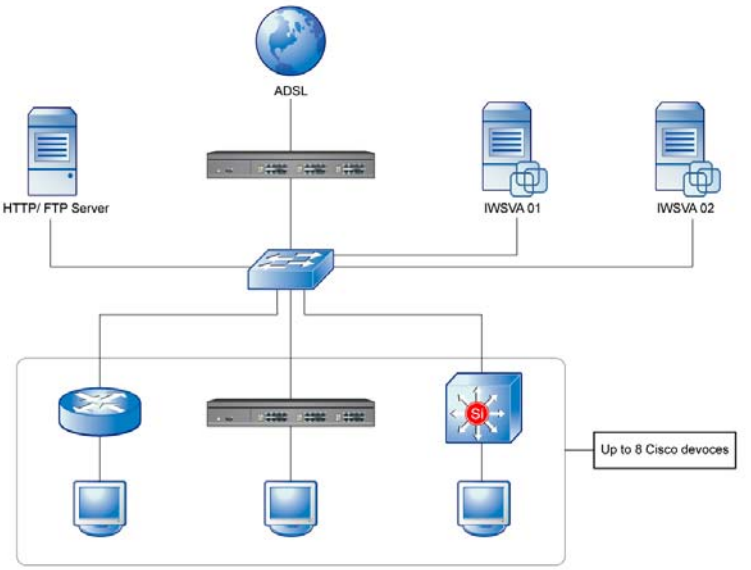


FIGURE 2-7 IWSVA deployment in a WCCP environment

Planning the HTTP Flow Using Forward Proxy Mode

For complete details on implementing Forward Proxy Mode, see Installing for Forward Proxy Mode on page 3-13.

HTTP Proxy in Standalone Mode

The simplest configuration is to install IWSVA in stand-alone mode, with no upstream proxy. In this case, IWSVA acts as a proxy server for the clients. Advantages of this configuration are its relative simplicity and that there is no need for a separate proxy server. A drawback of a forward proxy in stand-alone mode is that each client must configure the IWSVA device as their proxy server in their browser's Internet connection settings. This requires cooperation from your network users, and also makes it possible for users to exempt themselves from your organization's security policies by re-configuring their Internet connection settings.

Note: If you configure IWSVA to work in stand-alone mode, each client on your network needs to configure their Internet connection settings to use the IWSVA device and port (default 8080) as their proxy server.

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request, if the URL is not blocked. If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction. If the URL is valid, the HTTP service attempts to connect to the applicable Web server.
3. The contacted Web site returns a response from the Web server to the HTTP service.
4. The HTTP service scans the content for unwanted data and returns the appropriate response to the client.

TABLE 2-3. HTTP Proxy in Standalone Mode

ADVANTAGE	LIMITATION
Simple to install and manage.	Slow connection reaches maximum allowed connections limit.

HTTP Proxy in Simple Transparency Mode

Multiple IWSVA servers can be installed to balance your network traffic and scanning load. In this installation example, a Layer 4 switch receives clients requests and then forwards them to the IWSVA servers.

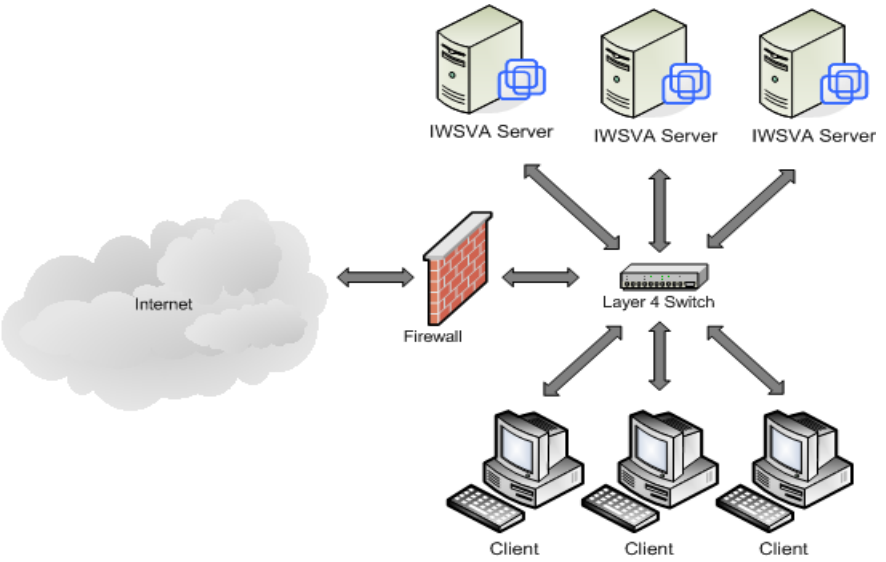
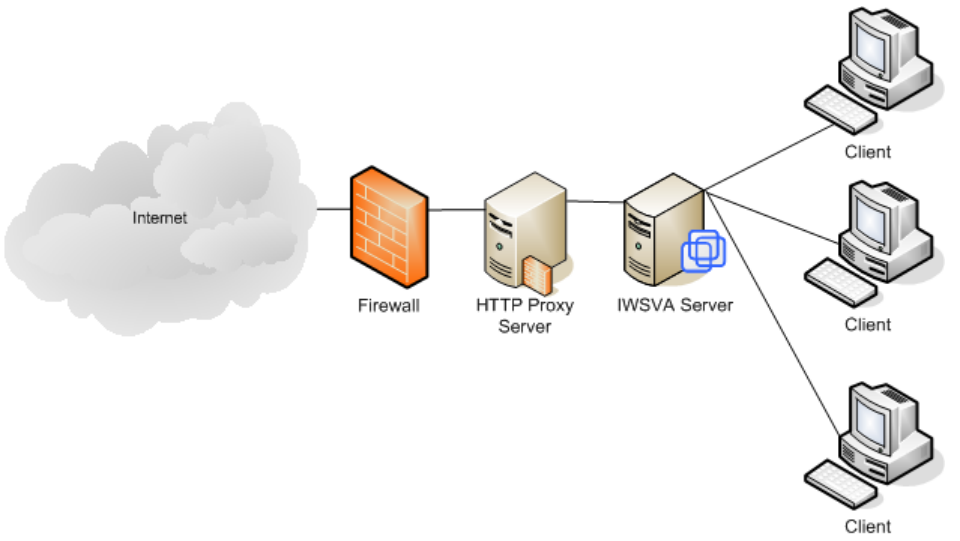


FIGURE 2-8 Use a Layer 4 switch to load balance between IWSVA servers in simple transparent mode

HTTP Proxy in Dependent Mode (Proxy Ahead)

For HTTP browsers to use this flow, configure the browsers to proxy through the IWSVA server, by default at port 8080.



HTTP Proxy in Dependent Mode (Proxy Ahead

Web page requests follow this sequence:

1. The Web client sends a request to the HTTP service.
2. The HTTP service validates the request.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to an upstream HTTP proxy server.
3. The upstream proxy server performs its processing, then forwards the request to the Web site on the Internet.
4. The contacted Web site returns a response (ideally a Web page) to the HTTP proxy server.
5. The HTTP proxy server performs its processing on the returned data, then forwards the response data to the IWSVA HTTP service.
6. The HTTP service scans the content for unwanted data and returns an appropriate response to the HTTP client.

TABLE 2-4. HTTP Proxy in Dependent Mode (Proxy Ahead)

ADVANTAGES	LIMITATIONS
Proxy server controls timing and content availability behavior.	IWSVA has to scan every response-even if cached.
It is more secure—configuration changes will affect cached objects.	
IWSVA does not wait for the downloading of already cached objects.	

HTTP Proxy in Dependent Mode (Proxy Behind)

The proxy behind flow consists of a caching proxy placed between the HTTP client and the IWSVA server without using ICAP. Organizations typically use this flow to increase performance, as with ICAP.

WARNING! Two security trade-offs exist for this potential performance enhancement:

1. If the cache contains data with a virus, for which there was no pattern when the data hit the cache, the IWSVA HTTP service cannot prevent the spread of the virus.

2. Similarly, if a policy regarding valid content changes, or unauthorized users request data that exists in the cache (for authorized users), the HTTP service cannot prevent subsequent unauthorized access to this data.

Instead of using the proxy-behind flow, Trend Micro recommends that administrators use an ICAP caching device. This solution provides the performance enhancements of caching without the security issues of proxy-behind topology.

Web page requests follow this sequence:

1. The Web client sends a request to HTTP proxy server.
2. The proxy server forwards the request to IWSVA.

3. IWSVA validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked), the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the Web server on the Internet.
4. The contacted Web server returns a response (ideally a Web page) to IWSVA.
5. IWSVA performs its processing on the returned data (virus, spyware, ActiveX scanning), then forwards the appropriate response/data to the proxy server.
6. The Proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

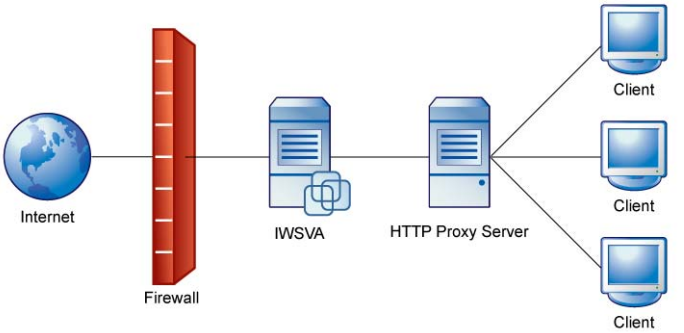


FIGURE 2-9 HTTP Proxy in Dependent Mode (Proxy Behind)

TABLE 2-5. HTTP Proxy in Dependent Mode (Proxy Behind)

ADVANTAGES	LIMITATIONS
No configuration changes required on the clients.	Configuration changes or pattern updates on IWSVA does not affect cached objects.
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays.	

HTTP Double Proxy in Dependent Mode

Double proxy configuration requires two caching proxies. The first proxy is placed between the HTTP client and the IWSVA server, and other one is placed between the IWSVA server and the Internet. This is typically used to get the advantages of the two configurations of the dependent modes: Proxy-ahead and Proxy-behind.

Web page request follows this sequence:

1. The Web client sends a request to the first proxy server.
2. The first proxy server forwards the request to IWSVA.
3. IWSVA validates the request using URL Filtering/Blocking.
   - If the URL is invalid (blocked) the HTTP service sends the HTTP client an appropriate notice, completing the transaction.
   - If the URL is valid, the HTTP service forwards the request to the second proxy server.
4. The second proxy server performs its processing, then forwards the request to the Web server on the Internet.
5. The contacted Web server returns a response (ideally a Web page) to second proxy server.
6. The second proxy server caches the data (if cacheable), then delivers the response/data to IWSVA.
7. IWSVA performs its processing on the returned data (Virus, Spyware, ActiveX scanning), then forwards the appropriate response/data to the first proxy server.

8. The first proxy server caches the data (if cacheable), then delivers the response/data to the HTTP client.

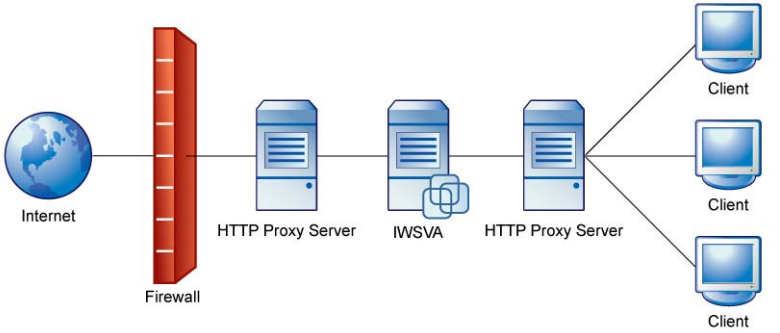


FIGURE 2-10 HTTP Double Proxy in Dependent Mode

TABLE 2-6. HTTP Double Proxy in Dependent Mode

ADVANTAGES	LIMITATIONS
Proxy server controls timing and content availability behavior.	Costs more—additional proxy server is needed.
IWSVA does not wait for the downloading of already cached objects.	
No configuration change required on the clients.	

HTTP Proxy in WCCP Mode (Single and Multiple IWSVA Servers)

IWSVA configured in WCCP Mode processes a Web page requests in the following sequence:

1. The Web client sends a request to the Web server.

2. The router intercepts the request and forwards the request to IWSVA.
3. IWSVA establishes a connection with the Web client.
4. IWSVA forwards the client requests to the Web server and establishes a connection with the Web server.
5. IWSVA begins sending data between the Web client and Web server.
6. If the data has no virus, then IWSVA sends the data to the Web client.
7. If the data has a virus, then IWSVA sends the blocked page to the Web client.

Deploying in ICAP Mode

Overview of ICAP Mode

Internet Content Adaptation Protocol (ICAP) is designed to forward an HTTP response or request to third-party processors and collect the results. The component that sends the ICAP request is called the *ICAP-client*. A component that processes the request is called an *ICAP-server*.

When IWSVA is configured in ICAP mode, it processes requests from any ICAP-compliant client. Officially, Trend Micro supports the following ICAP version

1.0 implementations: NetCache, Blue Coat, Cisco Content Engines (CE), and Squid 3.0.

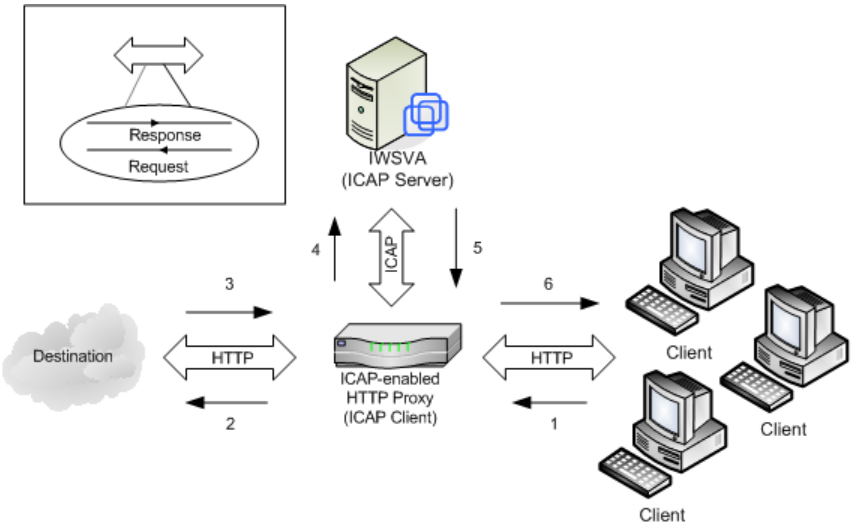


FIGURE 2-11 Using an ICAP-enabled Proxy

TABLE 2-7. ICAP-enabled Proxy

ADVANTAGES	LIMITATIONS
ICAP allows scanning of only new and necessary content.	Up front cost of ICAP equipment.
Reduced and selective scanning enhances performance	Adds extra steps in the IWSVA installation process.
Increased resource efficiencies reduce the number of IWSVA server hardware needed.	Requires management.

Planning the HTTP Flow Using ICAP Mode

For complete details on implementing ICAP Mode, see Installing for ICAP Mode on page 3-18.

HTTP Proxy in ICAP Mode (Single and Multiple IWSVA Servers)

This section discusses the flow of a typical HTTP GET request using both an ICAP device and IWSVA servers. In these flows, IWSVA interacts with the ICAP device, in response to ICAP rules. This is very different from other flows where IWSVA receives URL requests from HTTP clients. To use these flows for HTTP browsers, configure the browsers to use the ICAP device as the HTTP proxy.

Using ICAP devices can enhance performance in two ways:

- **Caching good data**–If the data is clean, the ICAP device caches the data. Subsequent requests require only four steps, not eight. (ICAP must still ask IWSVA to check the policies to validate that the users making the subsequent requests can browse the data, have not exceeded their quota, and so on.)
- **Clustered IWSVA servers**—When multiple IWSVA servers are used, the ICAP device load balances the requests between the servers. This is vital for enterprise environments where the demand for scanning incoming pages can overwhelm a single IWSVA server. With ICAP, the ICAP device performs load balancing, and receives maximum performance from the available IWSVA servers.

Note: Non-ICAP environments can receive similar benefits by using multiple IWSVA servers. However, the administrator must utilize additional load balancing technology.

When IWSVA is configured in ICAP mode, it processes requests from any ICAP-compliant client. Trend Micro supports the following ICAP client implementations:

- NetCache
- Blue Coat
- Cisco Content Engines
- Squid 3.0

Although IWSVA performs the same filtering of URLs and scanning of data for unwanted content, the ICAP flow is so different from the other flows that it requires a completely different communications protocol. Administrators indicate which protocol (ICAP or non-ICAP) to use during post-installation configuration.

The following figures show the HTTP flow with single and multiple IWSVA servers. (Both images assume the requested data is not in the ICAP device's cache.) The ICAP service determines which IWSVA server receives the request in a multi-server environment.

IWSVA configured in ICAP Mode processes Web page requests in the following sequence:

1. An HTTP client makes a request for a URL, sending the request to the ICAP caching proxy device.
2. The ICAP device, based on its configuration, determines that the request must be forwarded to an IWSVA server. If multiple servers are available, it alternates in round-robin fashion for load balancing.
3. The IWSVA server validates the URL.
   - If the URL is not blocked, IWSVA sends the response to the ICAP device.
   - If the URL is invalid (blocked), IWSVA directs the ICAP device to send an appropriate response to the HTTP client and the transaction is complete.
4. If the URL is valid, the ICAP server requests the page from the Web site on the Internet.
5. The Web site on the Internet returns the requested page (or some other appropriate response).
6. If the page is returned, the ICAP device, based on its configuration, determines that an IWSVA server must scan the data. Again, if multiple servers are available, it alternates in round-robin fashion for load balancing.
7. The IWSVA server scans the results and returns an appropriate response to the ICAP device, based on whether the data is clean or contains unwanted content.
8. If the data is clean, the ICAP device returns said data to the HTTP client, and the ICAP device retains a copy of the data to satisfy future requests. If the data contains unwanted content, the ICAP device returns an appropriate error message

(dictated by IWSVA) to the HTTP client, and the ICAP device does not retain a copy for future requests.

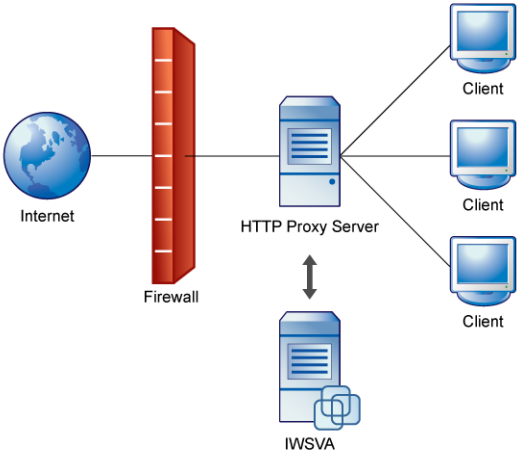


FIGURE 2-12 HTTP Proxy in ICAP Mode (Single IWSVA Server)

IWSVA ICAP Mode with Multiple Servers

If there is already a content cache server on your network, then Trend Micro recommends installing the ICAP HTTP handler. The following diagram shows the installation topology for IWSVA ICAP with multiple servers. For multiple IWSVA ICAP servers to work properly, their corresponding pattern, scan engine version, and `intscan.ini` files must be identical.

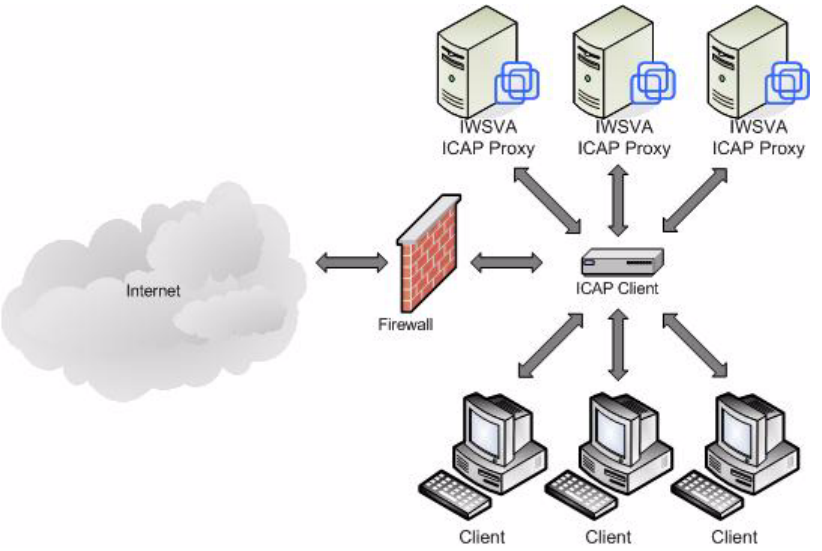


FIGURE 2-13 HTTP Proxy in ICAP Mode (Multiple IWSVA Servers)

TABLE 2-8. HTTP Proxy in ICAP Mode

ADVANTAGES	LIMITATIONS
No configuration changes required on the clients.	Configuration changes on IWSVA affect cached objects.
Cached objects are downloaded by clients directly from the Proxy server, which minimizes delays, and improves performance.	
Load-balancing possible after some configuration to the clients.	

Deploying in Reverse Proxy Mode

Overview of Reverse Proxy Mode

IWSVA is usually installed close to clients to protect them from security risks from the Internet. However, IWSVA also supports being installed as a reverse proxy to protect a Web server from having malicious programs uploaded to it. In Reverse Proxy Mode, IWSVA is installed close to the Web server that it protects. In this mode, IWSVA protects a Web server with the proxy server. The HTTP proxy is placed between the Internet and the Web server. This is useful when the Web server accepts file uploads from clients, or to reduce the load of each Web server by balancing the load among multiple Web servers. ASPs/ISPs can use IWSVA as an HTTP proxy to protect the upload traffic against viruses, and organizations with complex Web sites need it as a centralized point of access control.

IWSVA receives clients requests, scans all content and then redirects the HTTP requests to the real Web server. This flow is especially useful for Web sites involved in e-commerce transactions, distributed applications, which exchange data across the Internet, or other situations where clients upload files to the Web server from remote locations.

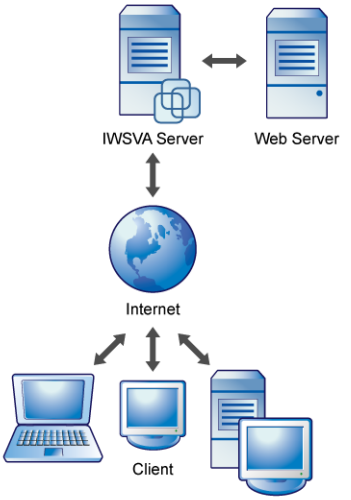


FIGURE 2-14 Reverse proxy protects Web server from clients

Planning the HTTP Flow Using Reverse Proxy Mode

For complete details on implementing Forward Proxy Mode, see Installing for Reverse Proxy Mode on page 3-21.

HTTP Reverse Proxy in Dependent Mode

In reverse proxy mode, the HTTP proxy acts as the Web server to the client systems. The proxy receives all requests and transfers them to the real Web server. Consequently, all HTTP traffic goes through the HTTP proxy, enabling the proxy to scan to content and block any infected transactions.

Note: Administrators should be aware of the following:
- The URL-filtering feature makes no sense in this configuration; only anti-virus scanning and URL-blocking are useful.
- In reverse proxy mode, the Web server's access log is useless. To analyze the connections for the Web site, you must use the IWSVA access log.

- Ideally, the reverse proxy server should be placed behind a firewall, but in many cases, the proxy is connected directly to the Internet, where it is more vulnerable to direct attacks. When a reverse proxy is configured without a firewall, administrators should take all appropriate precautions in securing the operating system hosting IWSVA.

IWSVA configured in Reverse Proxy Mode processes Web page requests in the following sequence:

1. Clients initiate the Web request.
2. The request is received by IWSVA, and configured to listen on port 80.
3. IWSVA scans the content, then forwards it to an actual Web server.
4. The Web server delivers the requested page back to IWSVA.
5. IWSVA rewrites the page headers, and sends on the request.
6. The modified page returns to the requestor.

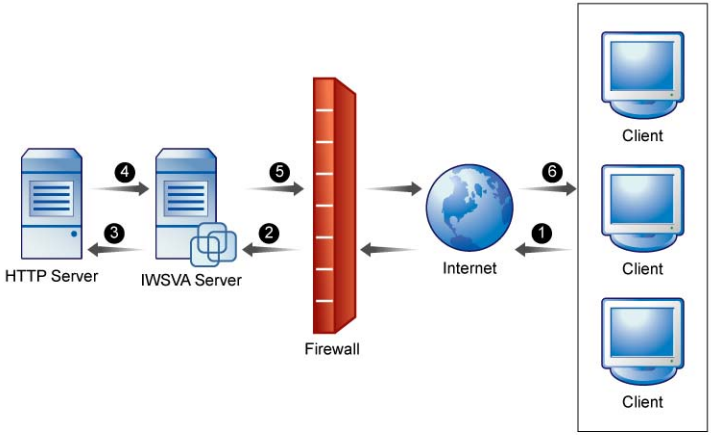


FIGURE 2-15 HTTP Reverse Proxy in Dependent Mode

TABLE 2-9. HTTP Reverse Proxy in Dependent Mode

ADVANTAGES	LIMITATIONS
IWSVA scans all objects only once-before they are cached.	New engines, patterns, and configurations will not affect cached objects.

TABLE 2-9. HTTP Reverse Proxy in Dependent Mode (Continued)

ADVANTAGES	LIMITATIONS
	Access logging feature of IWSVA is compromised.

Deploying in Transparent Bridge Mode

Overview of Transparent Bridge Mode

In Transparent Bridge Mode, IWSVA acts as a bridge between two network devices (switch, router, or firewall) and transparently scans HTTP(s) and FTP traffic. Transparent Bridge Mode is the simplest way to deploy IWSVA into an existing network topology and does not require modifications to clients, routers, or switches. IWSVA acts as a "bump in the wire" and scans for malware. Two network cards are required for IWSVA to be configured in Transparent Bridge Mode.

The benefit of Transparent Bridge Mode is that clients' HTTP(s) requests can be processed and scanned by IWSVA without any client configuration changes. This is more convenient for your end users, and prevents clients from exempting themselves from security policies by simply changing their Internet connection settings.

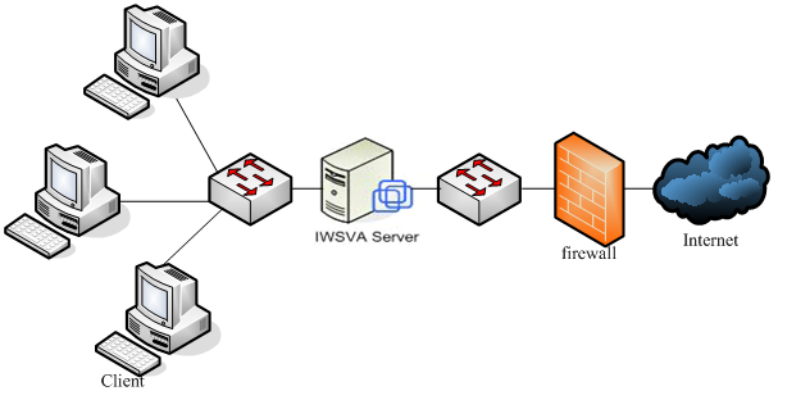


FIGURE 2-16 Typical bridge mode deployment

Planning the HTTP Flow Using Transparent Bridge Mode

For complete details on implementing Forward Proxy Mode, see Installing for Transparent Bridge Mode on page 3-11.

IWSVA configured in Transparent Bridge Mode processes a Web page requests in the following sequence:

1. The Web client sends a request to the Web server.
2. IWSVA accepts the connection from client and sends the request to the Web server.
3. IWSVA establishes a connection with the Web client.
4. IWSVA establish the connection with the Web server and gets data from the Web server.
5. If the data has no virus, then IWSVA sends the data to the Web client.
6. If the data has a virus, then IWSVA sends the blocked page to the Web client.

Chapter 3

Installing InterScan Web Security Virtual Appliance

This chapter explains the following:

- Operating System Requirements
- Component Installation
- Obtaining IWSVA
- Installing IWSVA
- Post-Installation Notes

Operating System Requirements

InterScan Web Security Virtual Appliance (IWSVA) provides a purpose-build, hardened and performance tuned 64-bit operating system as part of the installation process. This dedicated operating system installs with IWSVA to provide a turn-key solution—a separate operating system such as Linux, Windows, or Solaris is not required.

Component Installation

During installation, the following Trend Micro components are automatically installed:

- **Main Program**—Management console and the basic library files necessary for IWSVA.
- **HTTP Scanning**—Service necessary for HTTP scanning (either ICAP or HTTP proxy) and URL blocking.
- **FTP Scanning**—Service necessary for FTP scanning.
- **URL Filtering**—Service necessary for URL filtering requires a separate activation code.
- **Applets and ActiveX Scanning**—Service necessary for scanning Java applets and ActiveX controls. Requires a separate Activation Code.
- **IntelliTunnel Security**—Services to block communication provided by certain Instant Message (IM) protocols and certain authentication connection protocols.
- **SNMP Notifications**—Service to send SNMP traps to SNMP-compliant network management software.
- **Control Manager Agent for IWSVA**—Files necessary for the Control Manager agent. You need to install the agent if you are using Control Manager (Trend Micro's central management console).
- **Command Line Interface**—A custom CLI shell to manage IWSVA from the command line, either by TTY or SSH.

During installation, the following open-source application is installed for convenience, but is not enabled by default:

- **Squid 3.0**—To provide optional content caching.

Note: URL Filtering and Applets and ActiveX Scanning each require a separate activation code.

Obtaining IWSVA

IWSVA is supported on the following platforms:

- Bare Metal installation (dedicated off-the-shelf server platform without an operating system)
- VMware ESX or ESXi as a virtual machine

Trend Micro recommends that you evaluate the method of installation that best suits your environment.

You can install IWSVA from the Trend Micro Enterprise Solutions CD or download the installation ISO from the Trend Micro IWSVA download location (`http://www.trendmicro.com/download/product.asp?productid=86`). The CD is available to purchase and contains the installable file and all documentation.

To install from the Trend Micro Enterprise Solutions DVD

To complete this installation, you need to create a bootable installation CD with the IWSVA ISO file.

1. To create the installation media, insert the Trend Micro Enterprise Solution disk into the CD/DVD drive on the computer where ISO images can be created.
2. Copy the IWSVA ISO image from the Trend Micro Enterprise Solutions Media onto the local hard drive.
3. Eject the Enterprise Solutions CD and place a blank CD disk into the CD/DVD writer.
4. Burn the IWSVA ISO image to the blank CD.
5. Insert the newly created IWSVA Installation CD into the target server where you would like to install IWSVA.
6. Reboot the server and boot from the IWSVA installation CD to begin the installation process.

Note: The file on the Enterprise CD and on the Trend Micro Evaluation site is an ISO image. The ISO image allows you to create an IWSVA installation CD to install the product.

To download an evaluation version:

1. Go to the Trend Micro download Web page and download IWSVA.
   `http://www.trendmicro.com/download/product.asp?productid=86`
2. Download the IWSVA ISO.
3. Burn the IWSVA ISO image to the blank CD.
4. Insert the newly created IWSVA Installation CD into the target server where you would like to install the IWSVA application.

   WARNING! IWSVA does not support installation using an external USB CD/DVD drive.

5. Reboot the server and boot from the IWSVA installation CD to begin the installation process.

Note: The ISO image needs to be copied and then burned onto a blank CD in order to create the IWSVA installation CD (see the CD ISO creation document, *How to Use the Trend Micro IWSVA ISO File*).

Installing IWSVA

IWSVA only supports new installations or migrations from specific versions. In-place upgrades of an existing IWSS or IWSA installation is not supported.

IWSVA supports migrating existing configuration and policy data from IWSS 3.1 (Linux or Windows), IWSA 3.1 SP1, IWSVA 3.1, and IWSVA 5.0 products (see Migration on page 1-5). Existing log and report files are not migrated. If you need to retain existing IWSx 3.1 log and report information, please perform the necessary back up of these files before proceeding with the installation and migration.

The IWSVA installation process formats your existing system to install IWSVA. The installation procedure is basically the same for both a Bare Metal or a VMware ESX virtual machine platform. The Bare Metal installation simply boots off of the IWSVA installation CD to begin the procedure and the VMware installation requires the creation of a virtual machine before installation. The additional VMware virtual machine configuration is described in Appendix E, Creating a New Virtual Machine Under VMware ESX for IWSVA.

WARNING! **Any existing data or partitions are removed during the installation process. Backup any existing data on the system (if any) before installing IWSVA.**

IWSVA also installs a copy of the open source content caching application called *Squid*. It is disabled by default but you can enable this free open-source utility through the CLI interface. Trend Micro provides Squid content caching for convenience and easy installation. Support for Squid is provided by the Squid open-source community.

Trend Micro Disclaimer: Trend Micro IWSVA pre-installs Squid to help reduce the complexity of installing and configuring Squid to function with IWSVA. Squid is disabled by default and must be enabled by the customer through the IWSVA CLI after installation has been completed. Support for Squid is obtained through open source channels and it is the responsibility of the customer to become acquainted with Squid's benefits and functionality before enabling.

Additional information, documentation, and support on the Squid application can be found at the official Squid Web Proxy Cache Web site: `www.squid-cache.org`. Trend Micro will not provide support for Squid's features, but will provide support for the setup and integration of Squid and IWSVA through its CLI commands.

To install IWSVA:

1. Start the IWSVA installation.

Installing on a Bare Metal Server

Insert the IWSVA Installation CD (which was created from the IWSVA ISO image) into the CD/DVD drive of the desired server.

Note: Since IWSVA does not support external USB CD/DVD drives, a warning message “Cannot find kickstart file on CDROM" displays when installing IWSVA. You can safely ignore this warning message.

IWSVA does not support installation using an external USB CD/DVD drive.

Installing on a VMware ESX Virtual Machine

a. Create a virtual machine on your VMware ESX server

See Appendix E, Creating a New Virtual Machine Under VMware ESX for IWSVA.

b. Power on the virtual machine that was created to boot from the IWSVA installation ISO.

Note: If your computer boots from an ISO image (such as ISOLINUX), you need to press [ENTER] at the bootloader prompt to continue with the IWSVA installation process.

Installation Steps for both a VMware ESX Virtual Machine and a Bare Metal Server

A page appears displaying the IWSVA Installation Menu. The options in this menu as follows:

- **Install IWSVA**: Select this option to install IWSVA onto the new hardware or virtual machine.
- **System Recovery**: Select this option to recover an IWSVA system in the event that the administrative passwords cannot be recovered.
- **System Memory Test**: Select this option to perform memory diagnostic tests to rule out any memory issues.

- **Exit Installation**: Select this option to exit the installation process and to boot from the local disk.

2. Select **Install IWSVA**.

   The license acceptance page appears. From this page, you can access the readme (**Readme** button).

3. Click **Accept** to continue.

   A page appears where you choose a keyboard language.

4. Select the keyboard language for the system and then click **Next**.

   The IWSVA installer scans your hardware to determine if the minimum specifications have been met and displays the results illustrated as follows. If the host hardware contains any components that do not meet the minimum specifications, the installation program will highlight the non-conforming components and the installation will stop.

5. Select the deployment mode for the IWSVA installation and then click **Next**.

   Below are the deployment modes for the IWSVA installation. These are only enabled if you select a static IP address. Click **Edit** to set a static IP address.

   - Installing for Transparent Bridge Mode
   - Installing for Forward Proxy Mode
     - Standalone Proxy Configuration
     - Upstream Proxy Configuration
     - Simple Transparency using L4 Switch
     - Transparency using WCCP
   - Installing for ICAP Mode
   - Installing for Reverse Proxy Mode

6. Click **Next** to continue.

   A page appears where you specify network devices, hostname, and miscellaneous settings. If you choose to set the hostname manually, the Miscellaneous Settings will be available to you.

Note: You must assign a valid hostname to the IWSVA server for it to function properly.

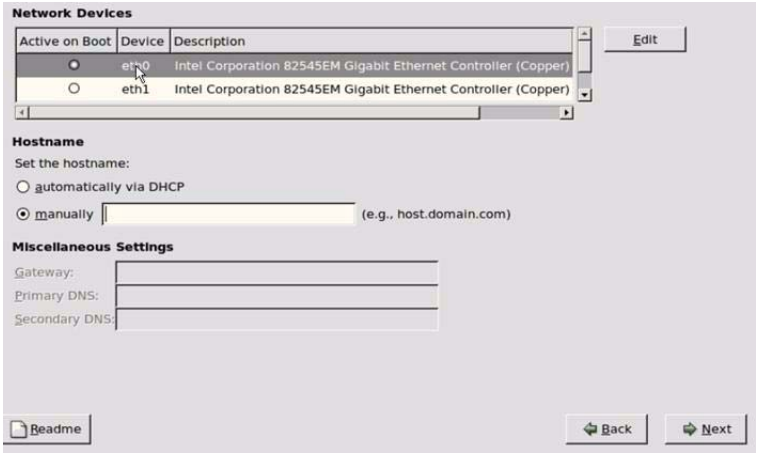


FIGURE 3-1 Page to specify network devices, hostname, and miscellaneous settings

7. Configure the network settings as required for IWSVA and then click **Next**.
8. From the time zone page, specify the time zone for IWSVA.

   Use the drop-down list to display the supported time zones or point to your location using the time zone map.
9. Click **Next**. A page appears where you specify the passwords for IWSVA.
10. Specify passwords for the root, enable, and admin accounts.

    IWSVA uses three different levels of administrator types to secure the system.

    The password must be a minimum of six characters and a maximum of 32 characters. For best security, create a highly unique password only known to you. You can use both upper and lower case alpha characters, numerals, and any special characters found on your keyboard to create your passwords.

    - **Root Account:** The Root account is used to gain access to the operating system shell and has all rights to the server. This is the most powerful user on the system.

- **Enable Account:** The Enable account is used to gain access to the command line interface's privilege mode. It has all rights to execute any CLI command.
- **Admin Account:** The Admin account is the default administration account used to access the IWSVA Web and CLI management interfaces. It has all rights to the IWSVA application, but no access rights to the operating system shell.

As you type the passwords, the password strength meter on the right indicates how strong the selected password is. For the best security, Trend Micro recommends using a strong, unique password.

11. Click **Next**.

A page appears where you accept all the configuration settings.

12. Confirm that the selected values are correct and then click **Next**.

The installation process prompts you to begin the installation. Selecting **Continue** erases any data on the hard disk partition and formats the hard disk. If you have data on the hard disks that you would like to keep, cancel the installation and backup the information before proceeding.

13. Click **Continue**.

A page appears that provides the formatting status of the local drive for the IWSVA installation. When formatting completes, the IWSVA installation begins.

After the installation is complete a summary screen appears. The installation log is saved in the `/root/install.log` file for reference.

14. Click **Reboot** to restart the system.

For a bare metal installation:

The CD automatically ejects. Remove the CD from the drive to prevent reinstallation.

For a virtual machine installation:

Trend Micro recommends disconnecting the CD-ROM device from the virtual machine now that IWSVA is installed.

After IWSVA reboots, the initial CLI login screen appears.

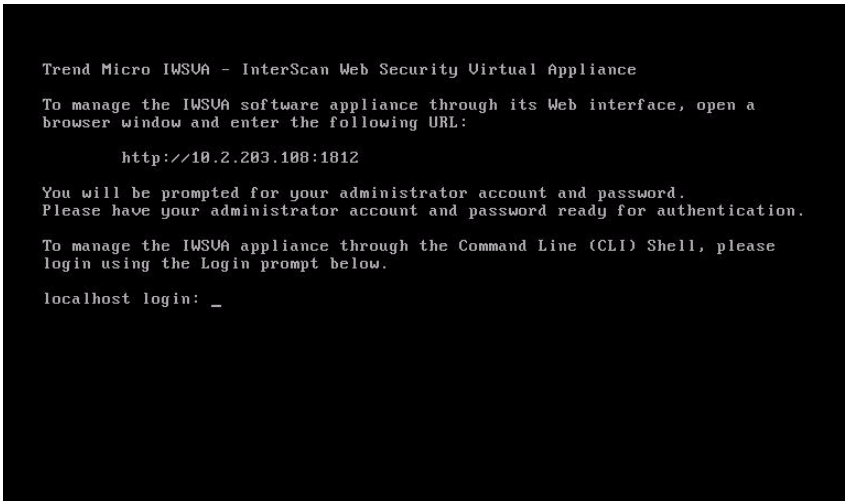


FIGURE 3-2 The initial CLI login screen

Note: During installation, you might receive the following messages:

```
for crash kernel (0x0 to 0x0) not within permissible range
powernow-k8: bios error -no psb or acpi_pss objects
```

Both of these messages are normal. The latter message indicates that the system BIOS is not reporting or presenting any PSB or ACPI objects or hooks to the Linux kernel. Either the CPU or BIOS does not support PSB or ACPI objects or hooks or they are simply disabled.

---

15. Log into either the CLI or the IWSVA Web console to launch IWSVA.

See Logging Into IWSVA for the First Time on page 3-23 for complete details.

Log into the CLI shell if you need to perform additional configuration, troubleshooting, or housekeeping tasks.

Choosing a Deployment Mode for the Installation

IWSVA can be deployed in different modes, depending on your network security needs.

Installing for Transparent Bridge Mode

Depending on the number of NIC cards detected, the Transparent Bridge Mode option might not be available. For Transparent Bridge Mode deployments, there must be a minimum of two detectable network cards in the system.

If you select **Deployment Option 1: Transparent Bridge Mode**, the following configuration information is required.

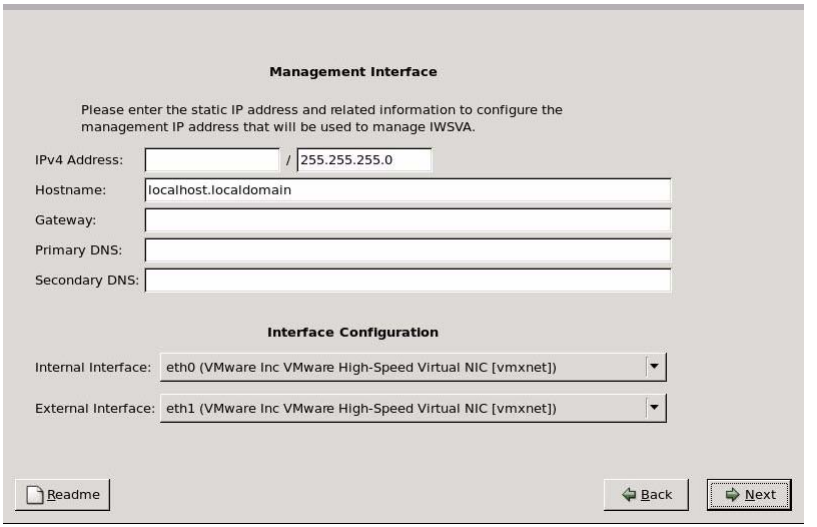


FIGURE 3-3 Page to specify the Transparent Bridge Mode configuration information

The table below describes the configuration information required for this deployment mode.

TABLE 3-1. Deployment Option 1: Transparent Bridge Mode

CONFIGURATION PARAMETER	DESCRIPTION
IPv4 Address	This is the IP address of the IWSVA management interface. Type in the IP address and appropriate subnet mask to complete the configuration.
Hostname	Type in the applicable FQDN hostname for this IWSVA host.
Gateway	Type in the applicable IP address to be used as the gateway for this IWSVA installation.
Primary DNS	Type in the applicable IP address to be used as the primary DNS server for this IWSVA installation.
Secondary DNS	Type in the applicable IP address to be used as the secondary DNS server for this IWSVA installation.
Internal Interface	Select which network adapter should be used for the internal connection of the transparent bridge.
External Interface	Select which network adapter should be used for the external connection of the transparent bridge.

Configuring Virtual Interface

In bridge mode, IWSVA supports virtual interface configuration on the data interface. If you want to set IWSVA to connect to the AU server or the rating server through the separate management interface, follow the proper configuration procedure described.

To configure a virtual interface:

1. Access the CLI (in enable mode) on the IWSVA server.
2. Configure the IP and gateway settings for the virtual interface on the data interface. In this example, the virtual interface IP address is 1.1.1.1, the subnet

mask is 255.255.255.0, and the gateway is 10. 168.160.254. The following shows the command example:

```
enable# configure ip static 1.1.1.1 255.255.255.0 10.168.160.254
```

3. Since the virtual interface is configured on the data interface, you will not be able to access the Web console through the data interface. You must enable the separate management interface through the CLI. Type the following command:

   ```
   configure mgmt interface eth2
   ```

4. Configure the IP settings for the separate management interface. The following shows the command example:

   ```
   enable# configure mgmt ip static 10.168.160.92 255.255.255.0
   ```

Installing for Forward Proxy Mode

If you select **Deployment Option 2: Forward Proxy Mode**, the following configuration information is required.

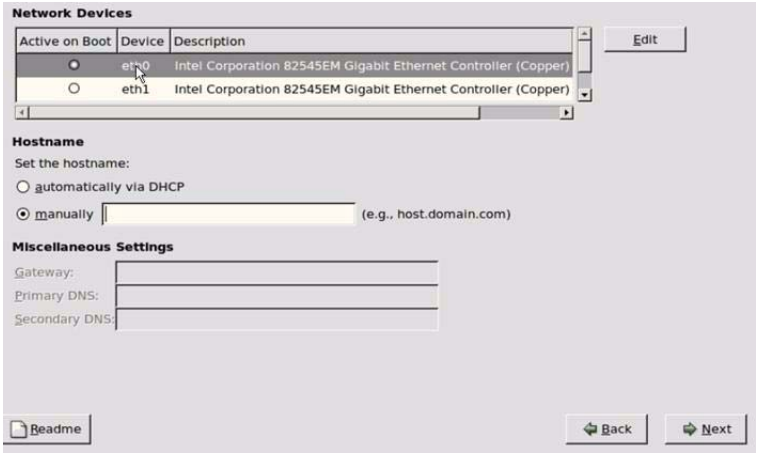


FIGURE 3-4 Page to specify the Forward Proxy Mode configuration information

The table below describes the configuration information required for this deployment mode.

TABLE 3-2. Deployment Option 2: Forward Proxy Mode

CONFIGURATION PARAMETER	DESCRIPTION
Network Devices	Configure the network interface card to use DHCP or manual IP address configuration.
Hostname	Select whether to set the hostname automatically through DHCP or manually. If set manually, type in the applicable FQDN hostname for this IWSVA host.
Gateway	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the gateway for this IWSVA installation.
Primary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the primary DNS server for this IWSVA installation.
Secondary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the secondary DNS server for this IWSVA installation.

- Click **Next** after the network configuration is set.

  An additional page appears where you specify the specific type of Forward Proxy Mode desired.

  Depending on the configuration information you supply, you can either specify Standalone Proxy Configuration, Upstream Proxy Configuration, Simple Transparency using L4 Switch, or Transparency using WCCP.

Standalone Proxy Configuration

TABLE 3-3. Standalone Proxy Configuration

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	8080
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Leave unchecked
Enable transparency	Enable / Disable simple transparency	Leave unchecked
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

Upstream Proxy Configuration

TABLE 3-4. Upstream Proxy Configuration

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	8080
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Check (enable)
Proxy Server	IP address of the upstream proxy server	Type in the value of the upstream proxy server
Port	Port of the upstream proxy server	Type in the port number of the upstream proxy server

TABLE 3-4. Upstream Proxy Configuration

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable transparency (check box)	Enable / Disable simple transparency	Leave unchecked
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

Simple Transparency using L4 Switch

TABLE 3-5. Simple Transparency using L4 Switch

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	80
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Leave unchecked
Enable transparency (check box)	Enable / Disable simple transparency	Check (enable)
Transparency Type	Select method of transparency	Select to use simple transparency
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

Transparency using WCCP

TABLE 3-6. Transparency using WCCP

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections	80
Enable upstream proxy (check box)	Enable / Disable upstream proxy	Leave unchecked
Enable transparency (check box)	Enable / Disable simple transparency	Check (enable)

TABLE 3-6. Transparency using WCCP

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Transparency Type	Select method of transparency	Select to use WCCP
Router IP address	Detail which router or switch to communicate with via WCCP	Type in the router or switch IP address
Password	Password for WCCP authentication	Type in the password for the WCCP authentication
WCCP forwarding method	This configures IWSVA to use the selected WCCP forwarding method	Select the GRE or L2 for WCCP forwarding method
Anonymous FTP over HTTP	The email address passed to FTP sites	Change to an appropriate address

- Click **Next** after completing the additional configuration information.

  A page appears where you specify your time zone. Proceed to Step 8 on page 3-8 to complete your time zone information.

Installing for ICAP Mode

If you select **Deployment Option 3: ICAP Mode**, the following additional configuration is required.

The table below describes the configuration information required for this deployment mode.

TABLE 3-7. Deployment Option 3: ICAP Mode

CONFIGURATION PARAMETER	DESCRIPTION
Network Devices	Configure the network interface card to use DHCP or manual IP address configuration.
Hostname	Select whether to set the hostname automatically through DHCP or manually. If set manually, type in the applicable FQDN hostname for this IWSVA host.
Gateway	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the gateway for this IWSVA installation.
Primary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the primary DNS server for this IWSVA installation.
Secondary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the secondary DNS server for this IWSVA installation.

- Click **Next** after the network configuration is set.

  An additional page appears where you specify additional ICAP Mode configuration information. Use the table below to complete the IWSVA configuration in ICAP Mode.

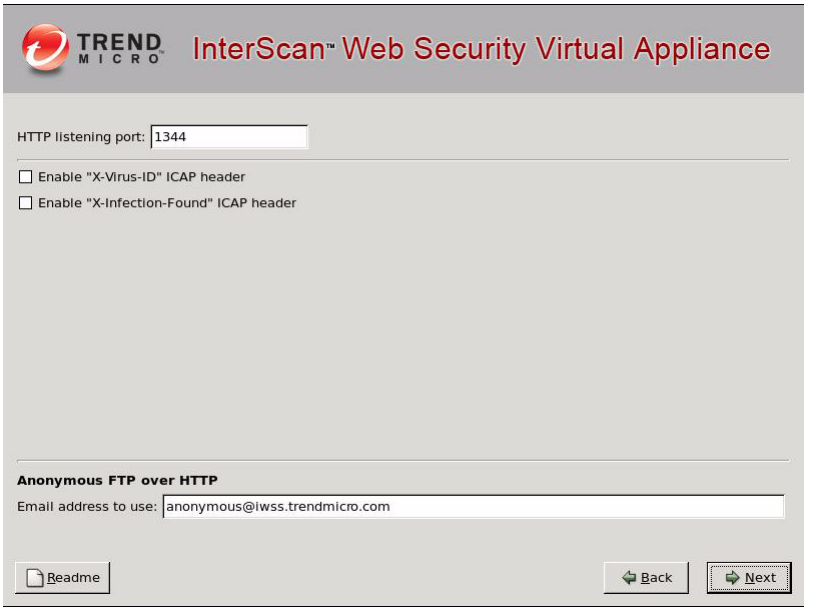


FIGURE 3-5 Page to specify additional ICAP Mode configuration information

The table below describes the configuration information required for this deployment mode.

TABLE 3-8. Deployment Option 3: ICAP Mode (Additional Information)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for ICAP.	1344

TABLE 3-8. Deployment Option 3: ICAP Mode (Additional Information)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
Enable X-Virus-ID (check box)	Enable / Disable ICAP details regarding malware detected being recorded.	Check (enable)
Enable X-Infection-Found (check box)	Enable / Disable ICAP details regarding malware detected and passing details back to the ICAP device.	Check (enable)
Anonymous FTP over HTTP	The email address passed to FTP sites.	Change to an appropriate address

- Click **Next** after completing the additional configuration information.

  A page appears where you specify your time zone. Proceed to Step 8 on page 3-8 to complete your time zone information.

Installing for Reverse Proxy Mode

If you select **Deployment Option 4: Reverse Proxy Mode**, the following additional configuration is required.

The table below describes the configuration information required for this deployment mode.

TABLE 3-9. Deployment Option 4: Reverse Proxy Mode

CONFIGURATION PARAMETER	DESCRIPTION
Network Devices	Configure the network interface card to use DHCP or manual IP address configuration.

TABLE 3-9. Deployment Option 4: Reverse Proxy Mode

CONFIGURATION PARAMETER	DESCRIPTION
Hostname	Select whether to set the hostname automatically through DHCP or manually. If set manually, type in the applicable FQDN hostname for this IWSVA host.
Gateway	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the gateway for this IWSVA installation.
Primary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the primary DNS server for this IWSVA installation.
Secondary DNS	If manual IP address configuration is selected for the network device, type in the applicable IP address to be used as the secondary DNS server for this IWSVA installation.

- Click **Next** after the network configuration is set.

  An additional page appears where you specify additional Reverse Proxy Mode configuration information. Use the table below to complete the IWSVA configuration in Reverse Proxy Mode.

The table below describes the additional configuration information required for this deployment mode.

TABLE 3-10. Deployment Option 4: Reverse Proxy Mode (Additional Information)

CONFIGURATION PARAMETER	DETAILS	RECOMMENDED VALUE
HTTP Listening port	This is the port that IWSVA listens on to receive connections for reverse proxy.	80
Protected Server	This is the IP address of the Web server IWSVA is protecting.	Type in the IP address of the protected server
Port	This is the SSL port of the Web server IWSVA is protecting.	Type in the SSL port number of the server being protected
Enable SSL Port (check box)	Enable / Disable SSL.	Leave disabled unless required
Anonymous FTP over HTTP	The email address passed to FTP sites.	Type in an appropriate email address

- Click **Next** after completing the additional configuration information.

  A page appears where you specify your time zone. Proceed to Step 8 on page 3-8 to complete your time zone information.

Logging Into IWSVA for the First Time

After IWSVA has restarted, you can log in to the appliance either through the CLI or the Web management interface.

- For the CLI interface, type in your administrator username and password at the console login prompt.

- For the Web management interface, on your workstation (not IWSVA) open a new Web browser and then type in the URL (http://<IWSVA 5.0 IP address>:1812) indicated in the initial CLI banner. You will need the IWSVA administrator account and password to login. The default administrator account name is “admin.”

Log in using the Web UI and perform the following tasks:

- Activate and license IWSVA with your activation keys.
- Update IWSVA with the latest scan engines and pattern files.

Post-Installation Notes

After IWSVA reboots and the initial CLI is available, Trend Micro recommends that you update your scan engine and virus pattern files immediately after registering and activating the product (see the Administrator’s Guide).

Chapter 4

Migrating to IWSVA

This chapter describes the following:

- About Migration
- Information Not Migrated
- Migrating from IWSS 3.1 Linux/Windows or IWSA 3.1 SP1 to IWSVA 5.0
- Migrating from IWSVA 3.1 to IWSVA 5.0
- Migrating from IWSVA 5.0 to another IWSVA 5.0

About Migration

IWSVA 5.0 supports both full and partial migration. Use full migration to restore system and application settings or to apply current configuration to an IWSVA replacement machine. Perform a partial migration if you want to replace policy and application level configurations.

WARNING! **IWSVA 5.0 does not support migration from another language version of IWSVA 5.0, IWSVA 3.1, IWSS 3.1 Linux/Windows, or IWSA 3.1 SP1.**

Before you perform a full migration, make sure the hardware configuration and deployment mode are the same on both the source and target IWSVA 5.0 machines.

Trend Micro recommends that you configure the target IWSVA 5.0 machine to use the same IP address as in the backup configuration file (exported from the source IWSVA 5.0 machine) to prevent unexpected behavior after a full migration.

Do NOT connect both IWSVA 5.0 machines to the network simultanously. Only one IWSVA 5.0 machine should be connected at a time.

The configuration and policy information for the following IWSVA products can be migrated to IWSVA:

- IWSS 3.1 Linux
- IWSS 3.1 Windows
- IWSA 3.1 SP1
- IWSVA 3.1
- IWSVA 5.0

Important Notes

- You can export IWSVA configuration to a backup file. Export information includes both system level and application level configuration settings.
- Use the **Config Backup & Restore** page in the Web console to import the backup file containing the IWSVA 5.0 configuration. A screen displays to prompt you to select either full migration or partial migration.

- Password information in a configuration backup file will not be displayed in clear text.
- IWSVA records a configuration import or export action in the audit log.

Information Not Migrated

The following lists the items that are not migrated.

Full Migration

- Logs stored in database, reports, messages, and quarantined files
- Pattern and engine files and related version information in configuration files
- Database password
- Product activation code
- HTTPS and applet re-sign CA certificates
- OS and application patch

Partial Migration

- Logs stored in database, reports, messages, and quarantined files
- Pattern and engine files and related version information in configuration files
- Database password and configuration
- Product activation code
- HTTPS and applet re-sign CA certificates
- Deployment mode configuration
- All configuration settings under the Administration menu in the Web console
- The following settings from IWSS3.1 Linux, IWSS3.1 Windows, IWSA 3.1 SP1 and IWSVA3.1:
  - Schedule reports
  - Log and report paths
- (For partial IWSVA 5.0-to-IWSVA 5.0 migration) System level settings such as IP address, hostname, and so on
- OS and application patch

Overview of the Migration Process

The following lists the major steps for both full and partial migration:

1. Back up previous IWSx settings for configuration rollback in case the migration process is not successful.
2. Perform a fresh IWSVA 5.0 installation on a new machine.
3. Import the previously backed up configuration file to the new IWSVA machine. If you are migrating from a source IWSVA 5.0 to a target IWSVA 5.0 machine, you can choose to perform a full or partial migration.
4. You can access the Web console to configure new IWSVA 5.0 features that are not in IWSVA 3.1, IWSS 3.1 Linux/Windows, or IWSA 3.1 SP1.

Note: After the migration process completes, the default settings apply for IWSVA 5.0 features that are not available in IWSVA 3.1, IWSS 3.1 Linux/Windows, and IWSA 3.1.

For a list of settings that are not migrated, refer to Information Not Migrated on page 4-3.

Migrating from IWSS 3.1 Linux/Windows or IWSA 3.1 SP1 to IWSVA 5.0

Note: IWSVA 5.0 does not support migration from another language version of IWSS 3.1 Linux/Windows, or IWSA 3.1 SP1.

1. Open the Web console of the source machine; then, select **Administration > Support**; then, click **Generate System Information File**.
2. Click **Download to your computer** to save the file to a local drive on your computer.
3. Open the Web console of the target IWSVA 5.0 machine and then select **Administration > Configuration Backup/Restore** from the main menu.
4. Click **Browse** to select a backup file and then click **Import**.

Migrating from IWSVA 3.1 to IWSVA 5.0

Note: IWSVA 5.0 only supports partial migration if you want to restore back to a previous backup IWSVA 3.1 configuration.

IWSVA 5.0 does not support migration from another language version of IWSVA 3.1.

1. Open the Web console of the source IWSVA 3.1 machine; then, select **Administration > Configuration Backup & Restore**, and then click **Export**.

   The screen displays a progress bar. When the export process is finished, a result page displays the status. If configuration export is successful, IWSVA opens a dialog box to prompt you to save the configuration file to a local disk. Save the file to a local drive on your computer.
2. Open the Web console of the target IWSVA 5.0 machine and then select **Administration > Configuration Backup & Restore** from the main menu.
3. Click **Browse** to select a backup file and then click **Import**.

Migrating from IWSVA 5.0 to another IWSVA 5.0

Note: IWSVA 5.0 does not support migration from another language version of IWSVA 5.0.

To perform a full migration, make sure the hardware configuration and deployment mode are the same on both IWSVA machines. Trend Micro also recommends you configure both machines to use the same IP address to prevent unexpected behavior after a full migration.

If the IP address information in the backup file is different from the IP address of the IWSVA machine to which you want to import the file, the migration results screen will not display. In this case, you can view the migration results in the Audit Log screen.

After a full migration, if the separate management interface is enabled on the source IWSVA 5.0 machine, you must use the management IP address of the source IWSVA 5.0 machine to access the Web console on the target IWSVA 5.0 machine.

1. Open the Web console of the source IWSVA 5.0 machine and select **Administration > Configuration Backup& Restore**. Then, click **Export** to back up the configuration.

   The screen displays a progress bar. When the export process is finished, a result page displays the status. If the configuration export process is successful, IWSVA opens a dialog box to prompt you to save the configuration file to a local disk. Save the file to a local drive on your computer.
2. Open the Web console of the target IWSVA 5.0 machine and then click **Administration > Configuration Backup/Restore** from the main menu.
3. Click **Browse** to select a backup file and then click **Import**.
4. A screen displays prompting you to select a full or partial migration. Choose an option and click **OK** to continue.

Appendix A

Deployment Integration

This appendix describes the following:

- IWSVA in a Distributed Environment
- Integration with LDAP
- Damage Cleanup Services (DCS) Integration
- Integration with a Cisco Router using WCCP
- Configuring the Cisco device and IWSVA for WCCP
- Configuring IWSVA for a WCCP Service Group
- Protecting an HTTP or FTP Server using Reverse Proxy
- Integration with an ICAP Device
- Configuring the Local Squid Proxy

IWSVA in a Distributed Environment

IWSVA is designed to be part of a distributed system and can establish a number of network connections based on the configuration settings.

The administrator must ensure the following:

- None of the required channels are blocked
- All channels have enough throughput
- Servers use a supported version of the software
- Servers are able to handle heavy traffic load

Connection Requirements and Properties

Table A-1 below provides the required connections and their properties.

TABLE A-1. Required Connections and Properties

CONNECTING COMPONENT	TRAFFIC: TYPE AND VOLUME	IF THE CONNECTION IS LOST
Clients	Should be measured on the real network	No protection
Database server	**Type:** TCP **Volume:** • **Low**—if access logging is disabled • **Medium**—if access logging is enabled	Cached data is used for already started services. Services will not start.
LDAP server (if configured)	**Type:** LDAP **Volume:** Medium	Cached data is used for already started services. Services will not start.
Trend Micro Active Update Server	**Type:** HTTP and HTTPS **Volume:** 10-50 Mb/day	IWSVA components cannot be updated in time.

TABLE A-1. Required Connections and Properties (Continued)

CONNECTING COMPONENT	TRAFFIC: TYPE AND VOLUME	IF THE CONNECTION IS LOST
Web Reputation	**Type:** HTTP **Volume**: Depends on the specific access	Cached data is used for already started services. Service will not start and user is given access to requested URL.
Trend Micro DCS server (if configured)	**Type:** HTTP **Volume:** Depends on the number of infected machines	No cleaning is performed for infected machines.

Throughput and Availability Requirements

The administrator must determine the IWSVA availability requirements.

- Is IWSVA downtime acceptable?
- If so, what is the proper action (bypass or stop) to enforce when IWSVA is down?
- If a failover configuration with multiple IWSVA instances is used, do the LDAP server and the database server have the same level of failover?

Integration with LDAP

Support Referral Chasing for Multiple LDAP Servers

IWSVA has an LDAP module that allows communication with multiple LDAP servers with the ability to establish multi-domain tree- and forest-like environments.

If the configured main LDAP server from the IWSVA Web console **Administration > Network Configuration > Deployment Mode | User Identification** page cannot resolve client credentials, and the "referral chasing" is enabled (providing that the referral server(s) is configured), IWSVA attempts to query for the requested User/Group object with the configured Primary Referral Server. If the queried object is still not found, a configured Secondary Referral will be queried. In order to do that, it must keep the credentials of the administrative account for all LDAP servers in the `[LDAP-Setting]` section of the `intscan.ini` file.

The Windows Active Directory (AD) Global Catalog enables LDAP clients, such as IWSVA, to query objects native to the domain being queried, and those residing in remote domains, as long as the AD server being queried and the remote AD server has Global Catalog enabled. The Global Catalog server accepts the LDAP requests on port 3268 and allows querying the user credentials, full name and membership in the global and universal groups across all other domains in the forest. The use of the Global Catalog is handy when creating IWSVA LDAP policies for a parent group with user(s)/group(s) member(s) residing on remote domains that are part of many sub-domain levels.

To use this feature, the IWSVA administrator should configure the main LDAP server that IWSVA uses from the Web console **Administration > Network Configuration > Deployment Mode | User Identification** page to communicate with a designated Global Catalog-enabled Active Directory server using port 3268, instead of using the default LDAP communication port 389.

Note: Global Catalog is only available in Microsoft Active Directory. The advantage of using the Global Catalog port includes better performance for LDAP object lookup, and allows object lookup that resides in many sub-levels of the Active Directory tree (beyond three). However, in order for IWSVA to utilize the Global Catalog, the AD being requested for an object needs to have the Global Catalog enabled along with the AD where the queried user/group object reside. IWSVA supports the use of the Global Catalog port only to be configured as the main LDAP server, and not part of the IWSVA referral chasing servers.

Tip: Trend Micro recommends allowing IWSVA to query the root Active Directory server with the Global Catalog enabled, and using Universal group types to do group nesting when applying policies. This can be seen by the Global Catalog and will be visible throughout the Active Directory. For more information, see Microsoft support (`http://support.microsoft.com/kb/231273`).

LDAP Authentication in Transparent Mode

Before configuring LDAP authentication on IWSVA deployed in transparent mode (bridge and WCCP), review the following criteria to ensure each item is fully met.

- IWSVA must have a valid hostname assigned (click **Administration** > **Network Configuration** > **Interface Configuration** | **Data Interface**). Make sure the hostname is also entered in the corporate DNS server.
- Ensure that the user ID cache is enabled. By default, this is enabled. If it has been disabled for any reason, it must re-enabled before enabling transparent mode authentication. You can enable user ID cache using the `configure ldap ipuser_cache enable` command in the CLI.
- By default, IWSVA keeps user ID cache information for up to 1.5 hours. If you need to lower the cache timeout value, use the `configure ldap ipuser_cache <interval>` command in the CLI to set a shorter cache interval.
- If authentication is enabled, IWSVA will block all non-browser applications trying to access the Internet. For example, the MSN application may try to access the Internet before the user has a chance to log in the IWSVA server. If this happens, the application will be blocked as the user has not successfully authenticated to IWSVA. You can perform one of the following:

  a. Bypass LDAP authentication for the application by adding the URLs that application accesses to "Global Trusted URLs." The URLs in this list will bypass both authentication and content scanning.

  b. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

  c. Add the IP address of the client machine to "LDAP authentication White List." IP address in this list will bypass LDAP authentication.

- When LDAP authentication is enable and you enable bridge mode on IWSVA and select **Enable transparence** in the Deployment Mode screen, a warning screen displays. This is because **Simple transparency** is selected by default and IWSVA does not support user/group name authentication in simple transparency mode. In this case, click **OK** to close the warning screen and select WCCP to use LDAP authentication.
- When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic

authentication feature provided in Internet Explorer Web browser. With automatic authentication, clients already logged on the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Note: You must configure IE settings to enable automatic authentication on each client computer.
By default, automatic authentication is enabled in IE 7.0.

Refer to the Administrator's Guide for more detailed information.

Damage Cleanup Services (DCS) Integration

While IWSVA can detect and block worms and spyware at the HTTP and FTP gateway, it can also work in conjunction with Trend Micro Damage Cleanup Services to clean infected clients. Damage Cleanup Services is a comprehensive service that helps assess and clean system damage without installing software on client computers in a network. It performs the following activities:

- Removes registry entries created by worms and Trojans
- Removes memory resident worms, Trojans, and spyware/grayware
- Repairs system file configurations modified by malware

After IWSVA is registered with one or more DCS servers, IWSVA issues a cleanup request if it detects one of the following trigger conditions:

- Client PC attempts to access a URL classified as "Spyware," "Disease Vector," or "Virus Accomplice" by the Phish pattern file, or
- Client PC uploads a virus classified as a worm

Note: If malware attempts to contact a remote server using a protocol other than HTTP, IWSVA will not detect it, thus will not trigger a cleanup.

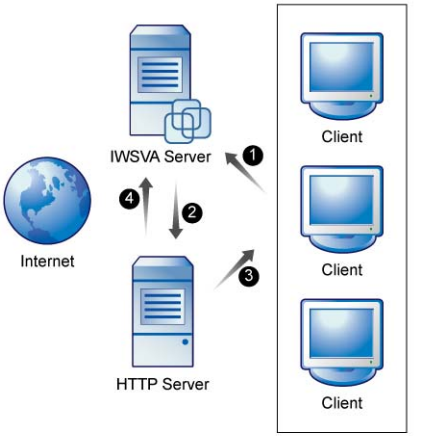


FIGURE A-1 How IWSVA requests DCS to perform a client cleanup

When IWSVA registers to a DCS server, infected client cleanups are handled in the following manner:

1. IWSVA detects the client attempting to access a URL listed in the PhishTrap pattern file or uploading a worm.
2. IWSVA requests the DCS server to clean up the infected client.
3. DCS attempts to connect to the infected client and clean it through remote procedures.
4. DCS reports the outcome of its cleaning attempt to IWSVA for logging.

When it receives a cleanup request from IWSVA, DCS attempts to connect to the infected client and repair the system damage. The outcome of the cleaning attempt, either successful or unsuccessful, is reported back to the IWSVA server for logging. If the cleanup attempt is not successful, then the client is redirected to a Web page hosted on the DCS server and an ActiveX control again attempts to clean the infected computer, with the permission of the computer's user.

Note: If you are using DCS in conjunction with a HTTPS-enabled IWSVA Web management console, IWSVA must be configured to allow access to the secure port (typically 8443). If access to the secure port is blocked, IWSVA will be unable to redirect clients to DCS for clean-up requests.

Using SSL with Damage Cleanup Services (DCS)

To redirect clients to DCS to clean up malicious code when you are using the HTTPS-enabled Web management console, access to the secure port that IWSVA uses (typically 8443) must be enabled. Otherwise, redirection to DCS will not be successful, because the redirection request will be blocked.

To allow access to secure port 8443:

1. Click **HTTP > Configuration > Access Control Settings**, and make the **Destination Ports** tab active.
2. Under the Action drop-down list, select **Allow.**
3. Select the **Port** radio button.
4. In the **Port** field, enter the port number used for HTTPS traffic (typically 8443).

5. Click **Add** and then **Save**.



FIGURE A-2 Allow access to the secure port (typically 8443) if using DCS and the HTTPS management console

Integration with a Cisco Router using WCCP

You can integrate IWSVA on a network that uses a Cisco router at the gateway without changing the browser settings of the client machines. This is achieved by utilizing Cisco's WCCP protocol.

Configuring the Cisco device and IWSVA for WCCP

In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSVA.

To configure a Cisco device and IWSVA for WCCP:

1. Configure WCCP on either the router or switch being used with IWSVA.

   Refer to your Cisco device manual for configuration details.

2. Log into the IWSVA Web console.
3. Click **Administration > Network Configuration > Deployment Mode**.
4. Select Forward Proxy.
5. Select Enable Transparency.
6. Select **Use Web Cache Coordination Protocol (WCCP)**.
7. Enter the router IP address(es).

   A maximum of eight routers can be entered. Enter only valid IP address(es).

8. Optionally, enter a password.

   If you specify no password for IWSVA, then you should specify no password for the router. If you specify a password for IWSVA, then ensure that the same password is also used for the Cisco device(s).

   While certain routers support Message-Digest algorithm 5 (MD5) encryption types 0-7, IWSVA only supports WCCP encryption types 0-6. Therefore, if you set the optional router password type for WCCP communication, choose a value from 0-6. Encryption type 7 is a Cisco proprietary type and is not supported.

9. Choose the WCCP forwarding method: GRE or Layer 2.

   Typically, Cisco routers only support GRE. Cisco switches only support the Layer 2 redirect assignment method. If in doubt, refer to the router or switch manual.

10. Click **Save** to save the WCCP settings.

After the WCCP configuration is saved, you can use the `show ip wccp 80 detail` command on the router or switch to verify that IWSVA has been added as one of the WCCP cache engines. If this addition is successful, various information displays, including the IWSVA IP address (Web Cache ID) and the state of the IWSVA unit, which will be usable. The following is a typical display indicating that IWSVA was added successfully:

```
Web Client ID:        10.204.170.97
Protocol Version:     2.0
State:                Usable
Redirection:          L2
Packet Return:        GRE
Packet Redirection:   55
Connect Time:         00:09:08
Assignment:           MASK
```

If IWSVA was not added successfully as one of the WCCP cache engines, then no information will be displayed. In this case, you can use the `debug ip wccp packets` command to determine the problem.

For IWSVA, certain WCCP communication-related information is also available from the `http.log` file in the `/etc/iscan/log/` directory. To locate this information, search for log entries that begin with "WCCP".

Note: The CLI command, `show log http <log date> monitor http` can be used to search for log entries.

To view WCCP logs, turn on the log flag (`wccp_logging = 1`) within the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.

Configuring WCCP Assignment Method

By default, the WCCP assignment method is mask. You can change this setting.

To configure WCCP assignment method:

1. From the shell, stop the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd stop
   ```

2. Modify the value of wccp_assignment_method in the /`var/iwss/IWSSPIProtocolHttpProxy.pni` file.

   The value 1 means hash and 2 means mask.

3. Restart the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd start
   ```

Configuring IWSVA for a WCCP Service Group

After installed, IWSVA uses service ID 80 (a WCCP component) to represent the WCCP service group. The associated router redirects HTTP/HTTPs and FTP traffic to this service group. In order to work with IWSVA, configure your routers using the same service ID. If a router does not have ID 80 available, then choose another service ID and then customize IWSVA as described in this section.

Load Balancing for WCCP Communication

Using the Well-Known Service Group for WCCP communication with more than one IWSVA device as part of the service group does not load balance as well as using the Dynamic Service Group (default service ID 80 for IWSVA). The load balancing offered by the Well-Known Service Group deviates more from the round robin concept than does the Dynamic Service Group. This might be because of the load balancing algorithm WCCP uses, and the way the WCCP router or firewall operates.

For best performance and resource usage distribution among IWSVA devices, Trend Micro recommends using the Dynamic Service Group (default service ID 80 for IWSVA) where applicable.

Note: In order to prevent communication related issues, WCCP needs to be configured on the Cisco router or switch before being configured on IWSVA (see Configuring the Cisco device and IWSVA for WCCP).

Configuring IWSVA to use the Dynamic Service Group

The WCCP's Dynamic Service ID is configurable by editing the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.

You can modify the following default entries from 80 to the desired service ID.

```
wccp_service=dynamic 80 protocol=tcp
flags=src_ip_hash priority=120 ports=80,21,443
```

Note: The first and second lines of the above code should be typed as a single line. Because of space limitations in this readme, this code occupies two lines.

To configure the Dynamic Service ID:

1. Access IWSVA though SSH or direct console.
2. Log in as root.
3. From the shell, stop the WCCP daemon by issuing the following command:

   `/usr/iwss/S99ISWCCPd stop`
4. Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by modifying the default service ID from 80 to the desired value.

   Example:

   ```
   wccp_service=dynamic 99 protocol=tcp
   flags=src_ip_hash priority=120 ports=80,21,443
   ```
5. Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.

   In the previous example, the configured service ID is 99.

6. From the console manager, restart the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd restart
   ```

Note: In order to implement the new service ID on IWSVA, restart the `wccpd` daemon after the service ID is modified. This results in both IWSVA and the supported WCCP Cisco device being configured to use the same service ID, which allows them to belong to the same service group. As members of the same service group, IWSVA and the WCCP Cisco device can communicate with each other.

The valid customizable WCCP Dynamic Service ID range is from 51-255, while 0-50 is reserved for Well-Known services. Certain WCCP routers only accept service ID range from 0-99.

Configuring IWSVA to use the Well-Know Service Group

For some older routers that do not support WCCP Dynamic Service group, IWSVA can be configured to use the Well-Known Service group.

Note: If IWSVA is configured to use the Well-Known Service ID to join a Well-Known Service group, then Trend Micro recommends configuring only one router on each IWSVA device.

To configure the Well-Known Service ID:

1. Access the IWSVA through ssh or direct console.
2. Log in as the `root` user.
3. Modify the following parameters in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file by commenting out the first line and then by adding the second one below:

   ```
   # wccp_service=standard 0 protocol=tcp
   flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120
   ports=80
   ```

   ```
   flags=src_ip_hash,dst_ip_hash,source_port_hash priority=120
   port=80
   ```

```
wccp_std_service=standard 0
```

4. Change the WCCP service ID on the WCCP-supported Cisco device to the configured service ID.

   In the previous step, the configured ID is 0. Typically, Cisco devices with WCCP support use the string, Web-cache, as part of the WCCP command for using service ID 0.

5. From the shell, restart the WCCP daemon by issuing the following command:

   ```
   /usr/iwss/S99ISWCCPd restart
   ```

Note: Based on the WCCP specification, the Well-Known service group configuration does not support FTP traffic redirection to IWSVA for scanning. Configure the WCCP Cisco device to use the Well-Known service type prior to configuring IWSVA to avoid WCCP communication issues.

Configuration 1: Firewall only between WCCP Router and Internet

The following graphic illustrates HTTP and FTP traffic.

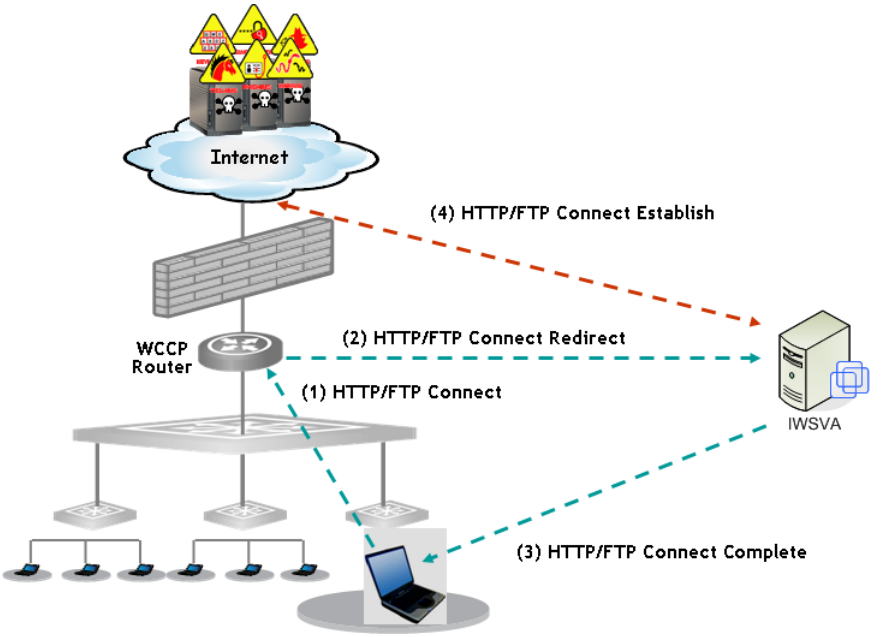


FIGURE A-3 WCCP and HTTP and FTP Traffic

Configuration 2: Firewall on Client Machine

If the client machine (laptop in the previous graphic) uses a personal firewall in addition to the firewall between the WCCP router and the Internet, then IWSVA cannot support FTP scanning.

Configuration 3: Stateful Firewall Between Client and IWSVA

If a stateful firewall exists between the client machine (laptop in the previous graphic) and IWSVA, then IWSVA cannot support FTP scanning.

Controlling WCCP Logging

HTTP and WCCP both write to the HTTP log. While HTTP uses the verbose attribute to enable or disable detailed logging, WCCP uses a different attribute to enable or disable logging.

By default, WCCP logging is enabled. You can disable WCCP logging by adding the line `wccp_logging=0` to the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file. Changing the line to `wccp_logging=1` turns WCCP logging back on again.

Configuration steps:

1. If the WCCP is already enabled, stop the WCCP daemon from the command line after accessing the IWSVA shell interface by `/usr/iwss/S99ISWCCPd` stop.
2. Add the line `wccp_logging=0 under the [http]` section in the `/etc/iscan/IWSSPIProtocolHttpProxy.pni` file.
3. Start the WCCP daemon from command line `/usr/iwss/S99ISWCCPd` start.

Note: WCCP logging only records WCCP control messages and not user traffic activities. The WCCP daemon needs to be restarted to pick up the WCCP logging settings in the `IWSVAPIProtocolHttpProxy.pni` file.

Sample PIX Firewall Configuration

Below, is an example of how WCCP could be configured on a PIX firewall using a Well-Known and Dynamic Service ID, along with an enabled password. The inside statement represents the name associated with an inside (most trusted) network interface on a PIX firewall.

The command lines containing Web-cache are used for a Well-Known Service ID. The command lines containing 80 are used for a Dynamic Service ID, with the default value for IWSVA specified. For more detailed PIX firewall configurations, refer to the relevant Cisco documentation.

```
wccp web-cache password <password>
wccp interface inside web-cache redirect in
wccp 80 password <password>
wccp interface inside 80 redirect in
```

The password is alpha-numeric and can be up to eight characters in length. The password is MD5-based and the same password specified for the firewall must be specified for IWSVA.

Protecting an HTTP or FTP Server using Reverse Proxy

If you are protecting the HTTP server, install the HTTP scanning service in the HTTP proxy mode and use the reverse proxy configuration.

- Define the following configuration setting in the [http] section of the pni-file
  - `self_proxy=reverse`—specifies operation mode
  - `reverse_server`—specifies the IP address of the protected HTTP server
  - `reverse_server_port`—specifies the TCP port of the protected HTTP server

Note: To simplify the deployment of the reverse-proxy configuration in an HTTP/HTTPS environment, IWSVA can listen for the incoming (HTTPS) connection on a port specified by the `[main]/secondaryport` configuration parameter, and forward this traffic without scanning to port 443 of the protected server.

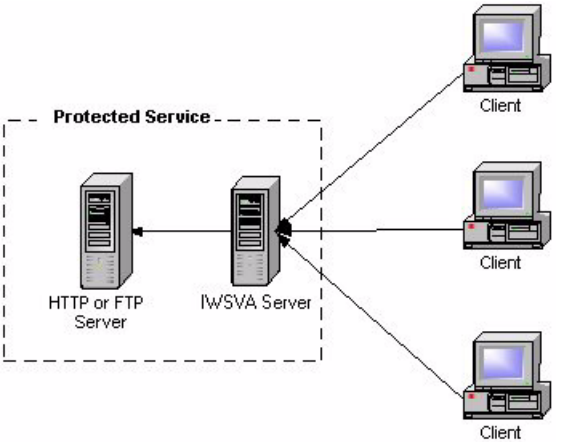


FIGURE A-4 Protecting a Dedicated Server

If you are protecting the FTP server, install the FTP scanning service and configure it to use an FTP proxy.

- Define the following configuration settings in the [ftp] section of the pni-file:

  - `proxy_mode=dedicated` specifies operational mode
  - `ftp_server` specifies the IP address of the protected FTP server
  - `ftp_server_port` specifies the TCP port of the protected server

Integration with an ICAP Device

You can integrate IWSVA on a network that utilizes an ICAP 1.0 compliant cache server.

Setting up an ICAP 1.0-compliant Cache Server

Configure an ICAP client to communicate with the ICAP server.

- To set up ICAP for NetCache Appliance: on page A-21
- To set up ICAP for the Blue Coat Port 80 Security Appliance: on page A-23
- To set up ICAP for Cisco CE ICAP servers: on page A-26

Setting up ICAP for NetCache Appliances

To set up ICAP for NetCache Appliance:

1. Log on to the NetCache console by opening `http://{SERVER-IP}:3132` in a browser window.
2. Click the **Setup** tab, and then click **ICAP** > **ICAP 1.0** in the left menu.
3. Click the **General** tab, and then select **Enable ICAP Version 1.0**. Click **Commit Changes**.

> **Note:** An error message `"icap: This service is not licensed."` appears if you have not provided the required ICAP license key for NetCache.

4. Enter an ICAP license key:
   a. Click the **Setup** tab, and then click **System > Licenses** in the left menu. The **System Licenses** screen appears.
   b. Type **IWFLPWA** under the **ICAP license** section.
   c. Click **Commit Changes**.
5. Select the **Service Farms** tab on the **ICAP 1.0** screen, and then click **New Service Farm** to add ICAP servers. Then, assign the service farm name in the **Service Farm Name** field.
   - For response mode, select **RESPMOD_PRECACHE** in the **Vectoring Point** field
   - For request mode, select **REQMOD_PRECACHE** in the **Vectoring Point** field
6. Select **Service Farm Enable**.
7. In the **Load Balancing** field, choose the proper algorithm that you use for load balancing (if you have more than one ICAP server in the service farm). Clear **Bypass on Failure**.

Note: Disable **Bypass on Failure** if the priority is more on virus propagation within your network. Otherwise, enable **Bypass on Failure** to guarantee an unblocked connection to the Internet.

8. Under the **Consistency** field, choose **strong** from the drop-down menu and leave the **lbw Threshold** field empty.
9. Under the **Services** text box (for response mode), type:
   `icap://{ICAP-SERVER-IP}:1344/resp on,`
   where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for response mode.

   Under the **Services** text box (for request mode), type
   `icap://{ICAP-SERVER-IP}:1344/REQ-Service on,`
   where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP for request mode.

   For multiple IWSVA ICAP server services, type the additional entries in step 8. For example:

   For response mode,
   - `icap://{ICAP-SERVER1-IP}:1344/resp on`
   - `icap://{ICAP-SERVER2-IP}:1344/resp on`

   Click **Commit Changes**.

   For request mode,
   - `icap://{ICAP-SERVER1-IP}:1344/REQ-Service on`
   - `icap://{ICAP-SERVER2-IP}:1344/REQ-Service on`

   Click **Commit Changes**.

Note: For multiple ICAP servers within a service farm with **strong** consistency selected, make sure that all ICAP servers have identical `intscan.ini` and other configuration files and the same virus pattern. The service farm will not work properly if the ICAP servers have different configurations.

10. Click the **Access Control Lists** tab, and then select **Enable Access Control Lists**.
11. Type `icap (Service Farm name of the ICAP Server) any` in the **HTTP ACL** field.
12. Click **Commit Changes**.

To configure scanning FTP over HTTP traffic, go to **FTP** > **Configuration** > **Access Control Lists**, and then add `"icap (service farm name)"` into the **FTP ACL** field.

Setting up ICAP for Blue Coat Port 80 Security Appliance

To set up ICAP for the Blue Coat Port 80 Security Appliance:

1. Log on to the management console by typing `http://{SERVER-IP}:8081` in the address bar of your Web browser (specifying port 8081 as the default management port).

   For example, if the IP address configured during the first-time installation is 123.123.123.12, enter the URL http://123.123.123.12:8081 in the Web browser.
2. Select **Management**. Type the logon user name and password if prompted.
3. Click **ICAP** in the left menu, and then click the **ICAP Services** tab.
4. Click **New**. The **Add ICAP Service** screen appears.
5. In the **ICAP service name** field, type an alphanumeric name and then click **OK**.
6. Highlight the new ICAP service name and click **Edit**.

   The **Edit ICAP Service name** screen appears.
7. Type or select the following information:
   a. ICAP version number (that is, 1.0)
   b. The service URL, which includes the virus-scanning server host name or IP address, and the ICAP port number. The default ICAP port number is 1344.
      - Response mode:

      `icap://{ICAP-SERVER-IP}:1344`
      - Request mode:

      `icap://{ICAP-SERVER-IP}:1344/REQ-Service`

      where `ICAP-SERVER-IP` is the IP address of IWSVA ICAP.
   c. The maximum number of connections (ranges from 1-65535). The default value is 5.
   d. The connection timeout, which is the number of seconds the Blue Coat Port 80 Security Appliance waits for replies from the virus-scanning server. The range is an interval from 60 to 65535. The default timeout is 70 seconds.

e. Choose the type of method supported (response or request modes).

f. Use the default preview size (bytes) of zero (0).

g. Click **Sense settings** to retrieve settings from the ICAP server (recommended).

h. To register the ICAP service for health checks, click **Register** under the **Health Check Options** section.

8. Click **OK** and then click **Apply**.

Note: You can edit the configured ICAP services. To edit a server configuration again, select the service and click **Edit**. The examples used for configuring ICAP for Blue Coat is based on version 2.1.07. The settings might vary depending on the version of Blue Coat.

---

9. Add response or request mode policy.

The Visual Policy Manager requires the Java 2 Runtime Environment Standard Edition v.1.3.1 or later (also known as the Java Runtime or JRE) from Sun™ Microsystems, Inc. If you already installed JRE on your workstation, the Security Gateway opens a separate browser window and starts the Visual Policy Manager. The first time you start the policy editor, it displays an empty policy.

If you have not installed JRE on your workstation, a security-warning window appears. Click **Yes** to continue. Follow the instructions to install the JRE.

To add the response mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Click **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**.

If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Content Policy**.

The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Bypass ICAP Response Service** and click **Set**.

The **Add Object** screen appears.

g. Click **New** and select **Use ICAP Response Service**.

The **Add ICAP Service Action** screen appears.

h. Choose the ICAP service name under the **ICAP Service/Cluster Names** field. Enable **Deny the request** under the **On communication error with ICAP service** section. Click **OK**, and then click **OK** again.

i. Click **Install Policies**.

To add the request mode policy:

a. Select **Management**. Type the logon user name and password if prompted.

b. Select **Policy** in the left menu, and then click the **Visual Policy Manager** tab.

c. Click **Start**. If the **Java Plug-in Security Warning** screen appears, click **Grant this session**.

d. On the menu bar, click **Edit > Add Web Access Policy**.

The **Add New Policy Table** screen appears.

e. Type the policy name under the **Select policy table name** field. Click **OK**.

f. Under the **Action** column, right-click **Deny** and click **Set**.

The **Add Object** screen appears.

g. Click **New** and select **Use ICAP Request Service**. The **Add ICAP Service Action** screen appears.

h. Choose the ICAP service name under the **ICAP Service/Cluster Names** field.

i. Enable **Deny the request** under the **On communication error with ICAP service** section.

j. Click **OK**, and then click **OK** again.

k. Click **Install Policies**.

10. To check the current policy, go to the Policy screen, click the **Policy Files** tab, and then click **Current Policy**.

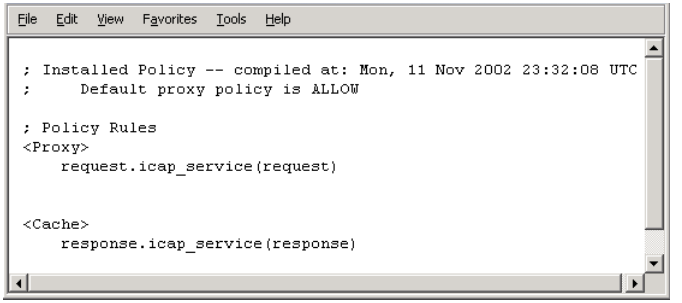


FIGURE A-5 Current configured policy

Setting up ICAP for Cisco CE ICAP Servers

IWSVA supports Cisco ICAP servers (CE version 5.1.3, b15). All ICAP settings are performed through a command line interface (CLI); there is no user interface associated with the Cisco ICAP implementation.

To set up ICAP for Cisco CE ICAP servers:

1. Open the Cisco CE console.
2. Type `config` to enter the configuration mode.
3. Type `ICAP` to display a list of all ICAP-related commands.
4. Create a response modification service, by typing the following:

   ```
   icap service RESPMOD SERVICE NAME
   ```

   The ICAP service configuration menu opens. Display a list of all available commands. Type the following commands:

   `server icap://ICAP SERVER IP:1344/resp` (to assign a server type)

   `vector-point respmod-precache` (to assign the proper vector point type)

   `error-handling return-error` (to assign the proper error-handling type)

   `enable` (to enable the ICAP multiple server configuration)
5. Type `exit`.
6. Create a request modification service, by typing

```
icap service REQUESTMOD SERVICE NAME
```

This command takes you into the ICAP service configuration menu. Display a list of all available commands. Issue the following commands:

`server icap://ICAP SERVER IP:1344/REQ-Service` (to assign a server type)

`vector-point reqmod-precache` (to assign the proper vector point type)

`error-handling return-error` (to assign the proper error-handling type)

`enable` (to enable the ICAP multiple server configuration)

7. Type `exit`.
8. For additional configuration steps, type the following:

   `icap append-x-headers x-client-ip` (to enable X-client headers for reports)

   `icap append-x-headers x-server-ip` (to enable X-server headers for reports)

   `icap rescan-cache ISTag-change` (to turn on ISTAG rescan for updates)

   `icap bypass streaming-media` (to exclude streaming media from ICAP scanning)

   `icap apply all` (to apply all settings and activate ICAP type)

   `show icap` (to display current ICAP configuration at root CLI menu)

Configuring Virus-scanning Server Clusters

For the Blue Coat Port 80 Security Appliance to work with multiple virus-scanning servers, you must configure a cluster in the Security Gateway (add the cluster, and then add the relevant ICAP services to the cluster).

To configure a cluster using the management console:

1. Select **Management**.

   Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click **New**.

   The **Add ICAP Cluster** screen appears.
4. In the **ICAP cluster name** field, type an alphanumeric name and then click **OK**.
5. Highlight the new ICAP cluster name and click **Edit**.

The **Edit ICAP Cluster name** screen appears.

6. Click **New** to add an ICAP service to the cluster.

   The **Add ICAP Cluster Entry** screen appears. The pick list contains a list of any services available to add to the cluster.

7. Choose a service and then click **OK**.
8. Highlight the ICAP cluster entry and click **Edit**.

   The **Edit ICAP Cluster Entry name** screen appears.

9. In the **ICAP cluster entry weight** field, assign a weight from 0-255.
10. Click **OK** and then **OK** again, and finally **Apply**.

Deleting a Cluster Configuration or Entry

You can delete the configuration for an entire virus-scanning server cluster, or you can delete individual entries from a cluster.

Note: Do not delete a cluster used in a Blue Coat Port 80 Security Appliance policy if a policy rule uses a cluster name.

To delete a cluster configuration using the management console:

1. Select **Management**. Type the logon user name and password if prompted.
2. Click **ICAP** in the left menu, and then click the **ICAP Clusters** tab.
3. Click the cluster you want to delete.
4. Click **Delete**, and then click **OK** to confirm.

Enabling “X-Virus-ID” and “X-Infection-Found” Headers

IWSVA can return 2 optional headers from the ICAP server whenever a virus is found: the “X-Virus-ID” and the “X-Infection-Found” headers. Neither of these headers are returned by default for performance reasons, because many ICAP clients do not use these headers. They must be enabled in the IWSVA management console.

- “X-Virus-ID” contains one line of US-ASCII text with a name of the virus or risk encountered. For example:

```
X-Virus-ID: EICAR Test String
```

- "X-Infection-Found" returns a numeric code for the type of infection, the resolution, and the risk description.

For more details on the parameter values, see:

`http://www.icap-forum.org/documents/specification/draft-stecher-icap-subid-00.txt`

To enable the X-Virus-ID header:

1. From the main menu, click **Administration** > **Network Configuration** > **Deployment Mode**.
2. On the **Deployment Mode** page, select **Enable 'X-Virus-ID' ICAP header** and/or **Enable 'X-Infection-Found' ICAP header**.

Configuring the Local Squid Proxy

See the Administrator's Guide for complete details.

Appendix B

Tuning and Troubleshooting

This appendix explains the following:

- IWSVA Performance Tuning
- Troubleshooting

IWSVA Performance Tuning

If you are experiencing issues with slow browsing performance, consider the following modifications and the IWSVA remote rating service.

URL Filtering

IWSVA utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the data supplied by the Trend Micro Web Reputation feature. Trend Micro recommends using the default setting of a weekly update check to ensure that your installation has the most current URL Filtering Engine.

IWSVA can control URL access based on Web Reputation feedback, the optional URL Filtering module, or a combination of both. The combination of Web Reputation and the URL Filtering module is a multi-layered, multi-threat protection solution provided by IWSVA.

The optional URL Filtering module grants or denies Web access based on the category to which a URL belongs. Web Reputation grants or denies Web access based on whether the requested URL is a phishing or pharming threat, has hacking potential, or has a reputation score that deems it untrustworthy. Both the optional URL Filtering module and Web Reputation are controlled by the specifications you make in policies.

For further details, see Chapter 7 in the Administrator’s Guide.

LDAP Performance Tuning

When running IWSVA to use the User/group name authentication identification method (LDAP), HTTP proxy performance becomes dependent upon the responsiveness of the LDAP directory server. In a worst case scenario, every HTTP request would require an LDAP query to authenticate the user's credentials, and another to retrieve group membership information for that user. These queries introduce latency in terms of the transmit/receive delay between IWSVA and the LDAP server, and add load to the LDAP server itself.

LDAP Internal Caches

To reduce the amount of LDAP queries required, IWSVA provides several internal caches:

- User group membership cache: This cache can store group membership information. By default, entries in this cache will be valid for 48 hours, or until the cache fills (at which point entries are replaced, starting with the oldest).

  The time to live (TTL) for entries in this cache can be configured through the setting `user_groups_central_cache_interval` in the [user-identification] section of `intscan.ini` configuration file.

- Client IP to User ID cache: This cache associates a client IP address with a user who recently authenticated from that same IP address. Any request originating from the same IP address as a previously authenticated request will be attributed to that user, provided the new request is issued within a configurable window of time (15 minutes by default for HTTP, 90 minutes for ICAP) from that authentication. The caveat is that client IP addresses seen by IWSVA must be unique to a user within that time period, thus this cache is not useful in environments where there is a proxy server or source NAT between the clients and IWSVA, or where DHCP frequently reassigns client IPs.

  To enable or disable this cache, change the `enable_ip_user_cache` setting in the [user-identification] section of the `intscan.ini` file. To change the TTL of this cache, change the `ip_user_central_cache_interval` (unit is hours). For example, to create a TTL of 30 minutes, enter `0.5`.

- User authentication cache: This avoids re-authenticating multiple HTTP requests passed over a persistent connection. When users pass the credential validation over a persistent connection, IWSVA adds an entry (two important keys in one cache entry are the client's IP address and the client's username) in the user authentication cache so the subsequent requests over a keep-alive connection will not authenticate again. The client IP address and client's username serve as two forward references, or links, to the "client IP to user ID cache" and "user group membership cache," respectively. IWSVA will thus still be able to retrieve the user's connection information from both the IP-user and user-group caches.

When deploying IWSVA with LDAP integration, it is important to consider the additional load that authenticating HTTP requests will place on the LDAP directory

server. In an environment that cannot effectively use the client IP to user ID cache, the directory server will need to be able to handle queries at the same rate as IWSVA receives HTTP requests.

Disable Verbose Logging When LDAP is Enabled

Trend Micro recommends turning off verbose logging in the `intscan.ini` file, under the [http] section, "verbose" parameter) when LDAP is enabled for server performance reasons. Verbose logging is primarily used by software developers to identify abnormal application behavior and troubleshooting. In a production deployment, verbose logging is usually unnecessary.

If verbose logging is enabled and LDAP is also enabled, IWSVA will log user authentication information and group membership information in the HTTP log in the \Log folder. Logs might contain hundreds of lines per user and therefore significantly consume disk space, depending on the amount of internal traffic and the number of groups a user is associated with. Verbose logging keeps the service busy with issuing I/O operations to the operating system. This might prevent the service from responding to HTTP requests in a timely fashion, hence latency might occur. In an extreme bursting HTTP traffic environment, it's possible to observe significant delays when IWSVA starts up in verbose mode.

LDAP Authentication in Transparent Mode

Before configuring LDAP authentication on IWSVA deployed in transparent mode, review the following criteria to ensure each item is fully met.

- IWSVA must have a valid hostname assigned (click **Administration** > **Network Configuration** > **Interface Configuration | Data Interface**). Make sure the hostname is also entered in the corporate DNS server.
- Ensure that the user ID cache is enabled. By default, this is enabled. If it has been disabled for any reason, it must re-enabled before enabling transparent mode authentication. You can enable user ID cache using the `configure ldap ipuser_cache enable` command in the CLI.
- By default, IWSVA keeps user ID cache information for up to 1.5 hours. If you need to lower the cache timeout value, use the `configure ldap ipuser_cache <interval>` command in the CLI to set a shorter cache interval.

- If authentication is enabled, IWSVA will block all non-browser applications trying to access the Internet. For example, the MSN application may try to access the Internet before the user has had a chance to log in the IWSVA server. If this happens, the application will be blocked as the user has not successfully authenticated to IWSVA. You can perform one of the following:

  a. Bypass LDAP authentication for the application by adding the URLs that application accesses to "Global Trusted URLs." The URLs in this list will bypass both authentication and content scanning.

  b. Instruct users to open their Web browsers and get authenticated before starting up applications that need Internet access.

  c. Add the IP address of the client machine to "LDAP authentication White List." IP address in this list will bypass LDAP authentication.

Note: When User/group authentication is enabled in either forward proxy mode or transparent mode with Active Directory, you can take advantage of the automatic authentication feature provided in Internet Explorer Web browser. With automatic authentication, clients already logged on the domain network can access the local Intranet without having to enter the logon information (such as the user name and password); that is, no password pop-up screen displays.

Please refer the IWSVA 5.0 Administrator's Guide for detailed configuration steps

---

Troubleshooting

Troubleshooting Tips

- **Issue:** IWSVA could not connect to the database specified in the Database Connection Settings page. The IWSVA management console displays the following error message:

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC] Could not connect to the
  server; Could not connect to remote socket.
  ```

  Solution:

  - Please check the ODBC connection or the database server and try again.

- **Issue:** The IWSVA management console displays an authentication error message.

  ```
  JDBC-ODBC BRIDGE: [UNIXODBC]FATAL: Password authentication
  failed for user.
  ```

  Solution:

  - Verify the user credential for the PostgreSQL Server and also ensure that the database settings are correct (**Administration > IWSVA Configuration > Database | Database Setting**). If the problem persists, ensure that the permissions in the `etc/iscan/odbc.ini` file are correct.

Before Contacting Technical Support

When contacting Technical Support with your issues, having specific information can streamline the process:

Installation Problems

Collect the following information about your installation problem before contacting Trend Micro technical support to expedite the process.

1. IWSVA version and build number
2. Screenshot of the exact error that appears during installation
3. The stage of the installation

General Feature Problems

If you have problems with IWSVA, collect the following information to give to Trend Micro support:

- The system file(s) that describes the current state of IWSVA.

  To compile these files, access the Web console and choose **Administration > Support** and then click **Generate System Information File**. This button is an extension of the Case Diagnostic Tool (CDT), allowing you to package the current machine "state" at a click of a button.

  The system file(s) that IWSVA generates from clicking the **Generate System Information File** button are packaged into a single file with the following format:

  `info_YYYYMMDD_999999.tar.tz`

  Where `YYYY` is the current year, `MM` is the current month, and `DD` is the current day that the package file was generated. `999999` is the UNIX time code.

  The system file(s) contains the following information:

  - **IWSVA information**—Includes IWSVA product version, engine version and build number, current pattern file (if available), and IWSVA hot fixes and service pack information. Product and integration settings are also part of this information
  - **IWSVA/system logs**—Includes IWSVA logs and debug logs, logs generated by syslogd daemon (if system logs are enabled), and core dump file
  - **System/network information**—Includes the hardware configuration, operating system, build, system resource status, other application installed, and network information
  - **CDT-compliant configuration/plug-ins information**—Includes information about changes made to CDT as a result of IWSVA adding a new component, such as a TMCM or MCP agent.

- Core files are first created in the first directory listed below, and then moved to the second directory listed:
  - `/etc/iscan/CoreDump`
  - `/etc/iscan/UserDumps`

  Use these files when working with Trend Micro technical support to help diagnose the cause of your problem. To view the files yourself, use a program like GDB, the GNU Project debugger.

- Log file for the day the issue occurred
  - All log files the day the issue occurred (logs are stored in `/etc/iscan/log` by default)
  - Make sure `verbose=1` is set in the [ftp], [http], and [notification] sections of the `intscan.ini` file
  - Make sure `log_trans=yes` is set under the [ftp] and [http] sections of the `intscan.ini` file
- From the Web console, take a screen shot of the **Summary** > **Scanning** tab page.
- Record the IWSVA version number.
- URL samples (if applicable)
- Get a packet capture of the failing transaction by using the CLI capture command (for example, enter `capture interface eth0` in enable mode).

Appendix C

Additional IWSVA Testing

This appendix describes the following:

- EICAR Test File
- Testing Upload Scanning
- Testing HTTPS Decryption Scanning
- Testing FTP Scanning
- Testing URL Monitoring
- Testing Download Scanning
- Testing URL Filtering
- Testing Spyware Scanning
- Testing PhishTrap
- Testing Java Applet and ActiveX Scanning
- Testing IntelliTunnel Security

EICAR Test File

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus appliance. This script is an inert text file. The binary pattern is included in the virus pattern file from most anti-virus vendors. The test virus is not a virus and does not contain any program code.

WARNING! **Never use real viruses to test your Internet security.**

Download the EICAR test virus from the following URLs:

`http://www.eicar.org/anti_virus_test_file.htm`

`https://secure.eicar.org/eicar.com`

Alternatively, you can create your own EICAR test virus by typing or copying the following into a text file, and then naming the file `eicar.com`:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H
*
```

Note: Flush the URL cache (**HTTP** > **Configuration** > **URL Cache**) and local browser before testing. If either cache contains a copy of the test virus, it's possible an attempt to download the file would get the file from the cache, rather than getting it from the Internet, and IWSVA would not detect the file.

Testing Web Reputation

To test IWSVA's Web Reputation feature, open a Web browser and type the following in the address field:

`http://wr21.winshipway.com`

If the test is successful, you should receive an IWSVA Security Event message stating, "This URL has a Web security rating that prohibits it from being accessed."

Testing Upload Scanning

The following procedure contains instructions to test uploading virus:

1. Open the IWSVA console and click **HTTP > HTTP Scan > Policies** in the main menu.
2. Clear **Enable virus scanning**, and then click **Save**.
3. Download the test virus (eicar.com) from the following page:

```
http://www.eicar.org/anti_virus_test_file.htm
```

4. Save the test virus on your local machine.
5. Re-open the IWSVA console, under **HTTP > HTTP Scan > Policies** in the main menu, select **Enable virus scanning**, and then click **Save**.
6. Upload the test virus to a Web site. A message similar to the following should display in your browser.

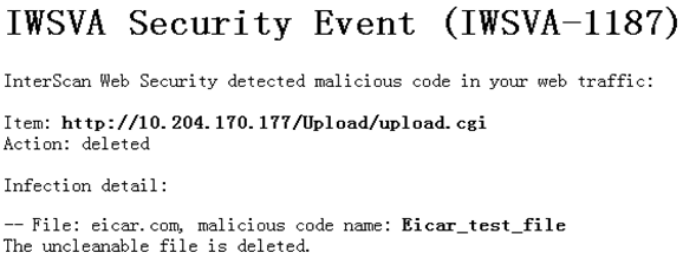


FIGURE C-1. This warning screen shows the detection of an EICAR test virus.

Testing HTTPS Decryption Scanning

This section describes the procedure to test HTTPS decryption on IWSVA in stand-alone mode.

To test virus scanning of decrypted HTTPS traffic:

1. Set the Web client's HTTP proxy to point to IWSVA (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).
2. Open the IWSVA Web console and click **HTTP > HTTPS Decryption > Settings | Server Certificate Validation** and make sure all options are selected.
3. Click **HTTP > HTTPS Decryption > Policies** and click **Enable HTTPS Decryption**.
4. Click **Add** to create a new HTTPS decryption policy. In the Rules tab, select **Disease Vector** under the Computers/Harmful category.
5. From the client machine, access the test virus file from the following URL:

```
https://secure.eicar.org/eicar.com
```

6. Since the server certificate is not in the trusted list on IWSVA, a certificate error notification displays. Click **Visit site anyway**.
7. A security warning screen displays. The warning message varies depending on whether URL filtering is also enabled or not.



FIGURE C-2 Security warning screen if URL filtering is disabled



FIGURE C-3 Security warning screen if URL filtering is also enabled

On the IWSVA server, you can view detail log information in the URL filtering log or the virus log.



FIGURE C-4 View the log for HTTPS decryption test in the Virus Log screen if URL filtering is disabled



FIGURE C-5 View the log for HTTPS decryption test in the URL Filtering Log screen if URL filtering is enabled

Testing FTP Scanning

The following procedure contains instructions to test FTP virus scanning in stand-alone mode.

To test virus scanning of FTP traffic:

1. Download the test virus from the following page:

   `http://www.eicar.org/anti_virus_test_file.htm`

2. Access the FTP server through IWSVA working as the FTP proxy.

For example, assume the following IP addresses: IWSVA FTP proxy server (`10.2.203.126`), FTP server (`10.2.202.168`).
Open a command line prompt and type the following:

```
ftp 10.2.203.126
```

3. Log on as `user@host`.

   For example, if your FTP account name is `anonymous` and the IP address of the FTP server is `10.2.202.168`; then, log on as `anonymous@10.2.202.168`

4. Upload the test virus (for example, eicar_com.zip) by typing the command

   ```
   put eicar_com.zip
   ```

5. If you have configured the IWSVA FTP proxy correctly, IWSVA displays a message similar to the following.

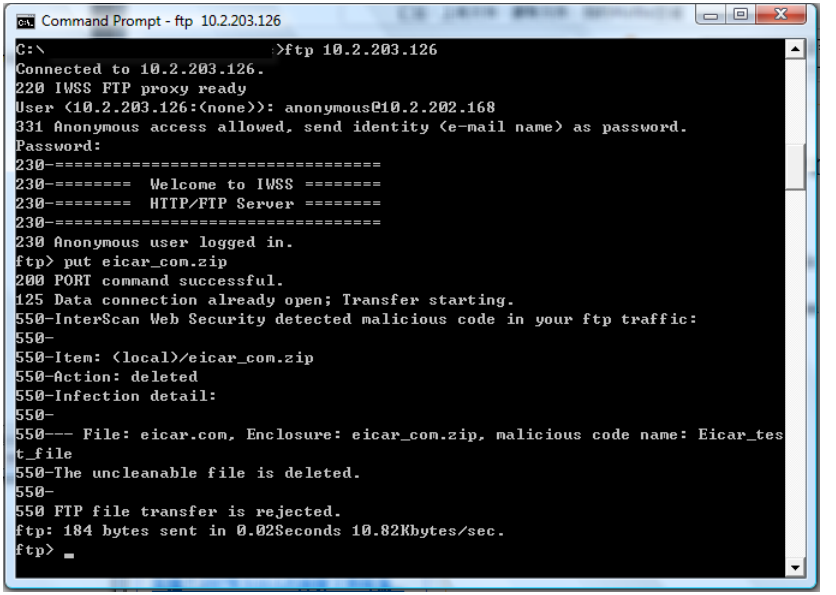


FIGURE C-6. This is a warning message that shows the detection of a virus in eicar_com.zip.

Testing URL Monitoring

Before testing the monitor feature in URL filtering, require your users to set the Web client's HTTP proxy to point to IWSVA.

- For stand-alone mode, set the Web client's HTTP proxy to point to IWSVA (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**).
- For upstream proxy, set the Web client's HTTP proxy to point to IWSVA (for example, open Internet Explorer and click **Tools > Internet Options > Connections > LAN Settings > Use a proxy server**). Open the IWSVA console and click **Administration > Network Configuration > Deployment Mode** and then check **Enable upstream proxy (dependent mode)**. Type the proxy address and the port number.

To test URL filtering:

1. Open the IWSVA Web console and click **HTTP > Configuration > Custom Categories** and create a new category "monitor" for the following URL:

   ```
   http://www.download.com
   ```

2. Click **HTTP > URL Filtering > Policies** and select **Enable URL Filtering**; then, click **URL Filtering Global Policy** to edit the policy.
3. In the Rule tab, select **Monitor** and click the check box under Leisure Time for "monitor" under Custom Categories; then, click **Apply**.
4. Select **Monitor** and click the check box under Leisure Time for Search Engines/Portals under Computers/Communications; then, click **Apply**.

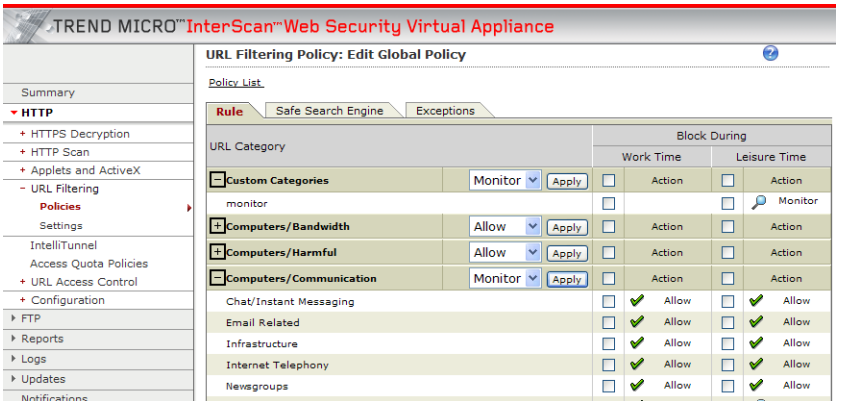


FIGURE C-7 Rule screen configuration for URL monitor testing

5. Save and deploy this policy.
6. From a client computer, access the following Web sites during leisure time:

   `http://www.download.com`

   `http://www.google.com`

   `http://www.yahoo.com`

You should be able to access the Web sites without seeing any warning messages. On the IWSVA server, you can query URL filtering logs for the Web access information.

Testing Download Scanning

To test virus scanning when downloading using HTTP or FTP over HTTP, attempt to download the test virus from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`

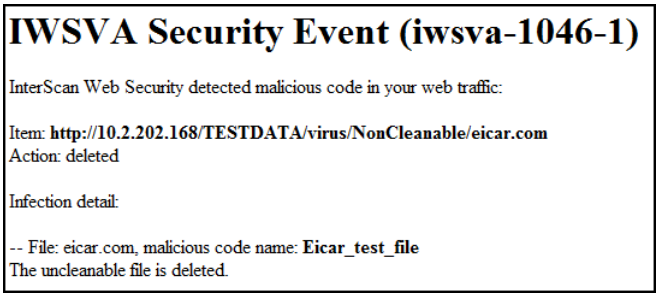


FIGURE C-8. The above virus-warning screen displays if the system is set up properly.

If a client attempts to download an infected file, IWSVA blocks other clients' access to that site for four hours by default. When other clients subsequently attempt to access the same URL that contained the virus, the user will see a URL blocking message instead of the virus-warning message.

Configure the default block time (in hours) by changing the parameter `infected_url_block_length` under the `[Scan-configuration]` section of the `intscan.ini` file.

Testing URL Filtering

Trend Micro recommends that you use the default settings to test URL filtering.

To test URL Filtering:

1. Click **HTTP > URL Filtering > Settings** from the main menu and in the **Schedule** tab. Configure the work days and times.
2. Click **HTTP > URL Filtering > Policies** from the Main menu.
3. Select **Enable URL filtering** and then click **Save**.
4. Click **URL Filtering Global Policy** and select the Block action to apply to the categories that you want blocked during work and leisure times.

   Keep the default settings in the Safe Search and Exception tabs.
5. Click **Save** to save any changes. Click **Deploy Policies** to make the policy effective immediately.

6. Open a browser and access any site that is in a category to be blocked at the time of the test.

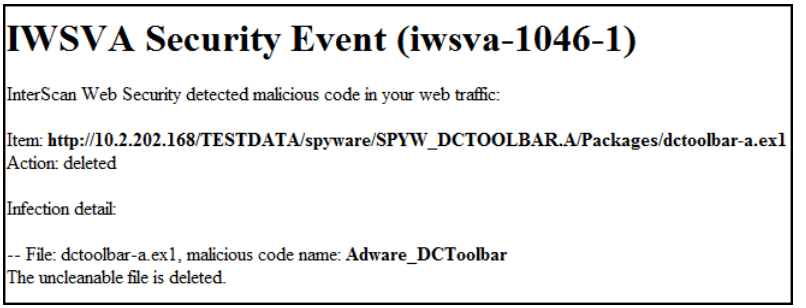
Testing Spyware Scanning

Perform the following procedure to test for spyware scanning.

To test Spyware scanning:

1. Open the IWSVA console and click **Summary**.
2. Click the **Scanning** tab.
3. Enable spyware and other grayware categories for scanning by clicking **HTTP scanning**.
4. Click **HTTP > HTTP Scan > Policies**.
5. Click **Virus Scan Global Policy**.
6. Click the **Spyware/Grayware Scan Rule** tab and then select the types of spyware/grayware which should be scanned.
7. Click **Save**.
8. Click **Virus Scan Global Policy**.
9. Click the **Action** tab.
10. Under the **Uncleanable files** field, select the action setting (Delete, Quarantine, or Pass).
11. Click **Save**.
12. Click **Deploy Policies**.

    After a successful spyware detection, a sample message appears:



IWSVA Security Event (iwsva-1046-1)

InterScan Web Security detected malicious code in your web traffic:

Item: **http://10.2.202.168/TESTDATA/spyware/SPYW_DCTOOLBAR.A/Packages/dctoolbar-a.ex1**
Action: deleted

Infection detail:

-- File: dctoolbar-a.ex1, malicious code name: **Adware_DCToolbar**
The uncleanable file is deleted.

FIGURE C-9. A sample message after detecting a spyware with action "Delete" setting.

Testing PhishTrap

Perform the following procedure to test PhishTrap.

To test Phishtrap scanning:

1. Open the IWSVA console and click **HTTP > URL Access Control > URL Blocking.**
2. Select **Enable URL blocking**.
3. Click the **Via Pattern File Phish** tab.
4. Under **Block the following Phish categories**, select all four categories (Phishing, Spyware, Virus accomplice, Disease vector).
5. Click **Save**.
6. After a successful phishing site detection, a sample message appears:

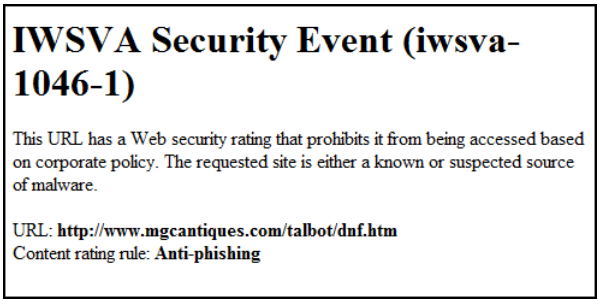


FIGURE C-10. A sample message after detecting a phishing site.

Testing Java Applet and ActiveX Scanning

Java applets and ActiveX controls are used on many Web pages to display interactive content or applications. One way to test your installation is to temporarily configure the global policy to block all applets and ActiveX controls, and then attempt to open Web pages that use them (to verify that the applet or object is blocked).

To test Java applet and ActiveX scanning:

1. Click **HTTP > Applets and ActiveX > Policies** from the main menu.
2. If necessary, select **Enable Applet/ActiveX security** and click **Save**.
3. Click **Applet/ActiveX Security Global Policy**.
4. On the **Java Applet Security Rules** tab, click **Block all Java applets** and then click **Save**.
5. Click **Applet/ActiveX Security Global Policy**.
6. On the **ActiveX Security Rules** tab, click **Block all cabinet files** and **Block all PE format files** and then click **Save**.
7. Click **Deploy Policies**.
8. Open a Web browser and attempt to navigate to Web sites that use Java applets and ActiveX controls.

   For example, for stock price tickers or games, IWSVA will block the mobile code from downloading and running in your browser.

Note: Blocking all Java applets and ActiveX controls might be too restrictive for your environment because it will prevent many legitimate Web sites from functioning properly. After testing, Trend Micro recommends going back to the **Applets and ActiveX Policy: Edit Global Policy** screen to change the settings back to the default or your own less-restrictive configuration.

Testing IntelliTunnel Security

To test IntelliTunnel security:

1. Download the latest MSN Messenger from `http://get.live.com/messenger/overview`
2. Install MSN Messenger.
3. Enable IntelliTunnel in IWSVA.
   a. Click **HTTP** > **IntelliTunnel**.
   b. Create a new policy or open an existing one.
   c. Select **Microsoft Messenger (MSNP Protocol)**.
   d. Click **Save**.
   e. Select the policy and then click **Deploy Policies**.
4. Configure proxy settings in Internet Explorer.
   a. Open Internet Explorer.
   b. Click **Tools** > **Internet Options**.
   c. Click the **Connections** tab.
   d. Click **LAN Settings**.
   e. Select **Use a proxy for your LAN**. These settings will not apply to dial-up or VPN connections.
   f. Enter the IWSVA IP address in the **Address** field.
   g. Enter the IWSVA HTTP listening port in the **Port** field. This value must match **Administration** > **Network Configuration** >**Deployment Mode** > **HTTP Listening Port** in IWSVA.

h. Click **OK** and then **OK** again.

i. Close Internet Explorer.

5. Login to MSN Messenger.

   An error message should appear stating that you were not able to sign into Windows Live Messenger at this time.

6. Disable IntelliTunnel.

   a. Click **HTTP > IntelliTunnel**.

   b. Open the policy.

   c. De-select **MSN Messenger**.

   d. Click **Save**.

   e. Select the policy and then click **Deploy Policies**.

7. Login to MSN Messenger.

   MSN Messenger should now work.

Note: MSN Messenger uses the proxy configuration in Internet Explorer, so this test should be valid without requiring any modifications to firewalls, network, etc. Other IM applications might not honor the proxy configuration in Internet Explorer and only fall back to port 80 if the standard port is blocked.

Appendix D

Maintenance and Technical Support

This appendix describes the following:

- Product Maintenance
- Contacting Technical Support
- Security Information Center
- Click Security Info from the drop-down menu at the top-right panel of the screen. The Security Information screen displays.

Product Maintenance

From time to time, Trend Micro might release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

`http://www.trendmicro.com/download/`

The Update Center screen displays. Select your product from the links on this screen:

Clicking the link for InterScan Web Security Virtual Appliance takes you to the Update Center page for IWSVA. Scroll down to review the patches that are available.

Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Note: If the Maintenance Agreement expires, your License Agreement will not.

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

```
https://olr.trendmicro.com/registration/
```

Renewing Your Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company's Registration Profile.

To view or modify your company's Registration Profile, log on to the account at the Trend Micro online registration Web site:

```
https://olr.trendmicro.com/registration
```

You are prompted to enter a logon ID and password.

To view your Registration Profile, type the logon ID and password created when you first registered your product with Trend Micro (as a new customer), and then click **Log on**.

Contacting Technical Support

To contact Trend Micro Technical Support, visit the following URL:

`http://kb.trendmicro.com`

Then, click the link for one of the following regions:

- Asia/Pacific
- Australia and New Zealand
- Europe
- Latin America
- United States and Canada

Follow the instructions for contacting support in your region.

In the United States, Trend Micro representatives can be reached through phone, fax, or email. Our Web site and email addresses follow:

`http://www.trendmicro.com`

`support@trendmicro.com`

For regional contact information and the specific technical support numbers for all the regional and worldwide offices, open the IWSVA management console and choosing **Support** from the menu in the management console's banner.

General US phone and fax numbers follow:

```
Voice: +1 (408) 257-1500 (main)
```

```
Fax: +1 (408) 257-2003
```

Our US headquarters is located in the heart of Silicon Valley:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support.

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

`http://kb.trendmicro.com`

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question through an email message. Response time is typically 24 hours or less.

Known Issues

Known issues are features in your IWSVA software that might temporarily require a workaround. Known issues are typically documented in section 7 of the Readme document you received with your product. Readme files for Trend Micro products, along with the latest copies of the product manuals, can also be found in the Trend Micro Update Center:

`http://www.trendmicro.com/download/`

Known issues can be found in the technical support Knowledge Base:

`http://kb.trendmicro.com`

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

`http://subwiz.trendmicro.com/SubWiz`

Click the "Submit a suspicious file/undetected virus" link. The following screen displays.

You are prompted to supply the following information:

- **Email**: Your email address where you would like to receive a response from the antivirus team.
- **Product**: The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats**: The number of users in your organization that are infected.
- **Upload File**: Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word "virus" as the password—then select the protected zip file in the **Upload File** field.
- **Description**: Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any risks it might contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

If you prefer to communicate by email, send a query to the following address:

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:

`(877) TRENDAV, or 877-873-6328`

Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

`http://www.trendmicro.com/vinfo/`

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- View a Virus Map of the top 10 risks around the globe
- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
    - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
    - The Trend Micro *Safe Computing Guide*
    - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low vs. Medium or High risk
    - A glossary of virus and other security risk terminology

- Download comprehensive industry white papers
- Subscribe, free, to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters
- Read about TrendLabs, Trend Micro's global antivirus research and support center

To open Security Information:

1. Open the IWSVA management console.
2. Click **Security Info** from the drop-down menu at the top-right panel of the screen. The **Security Information** screen displays.

Appendix E

Creating a New Virtual Machine Under VMware ESX for IWSVA

This appendix describes how to create a new virtual machine for IWSVA.

Creating a New Virtual Machine

The actual installation of ESX 3.5.0 is not covered in this document. Please refer to VMware's product documentation to install this product.

The steps outlined below detail the process to create a new virtual machine under VMware ESX to install IWSVA. Please use the following steps as a guideline for creating the virtual machine for your environment. The number of CPUs, NIC cards, memory and hard disk space selected should reflect the requirements for your deployment. The values entered here are for instructional purposes.

To load the IWSVA installation ISO to the VMware server's hard disk

1. Open the VMware Virtual Infrastructure client and click the **Configuration** tab.
2. From the **Hardware** area, click **Storage**.
3. In the **Storage** area, double click a storage area that contains enough space to upload the IWSVA ISO.

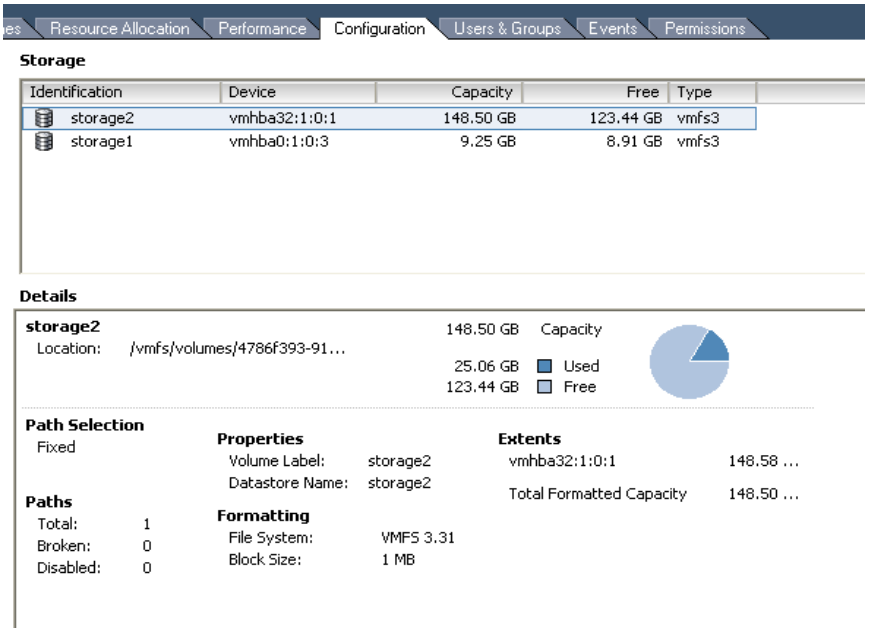


FIGURE E-1 Configuration Tab

The Datastore Browser window opens.

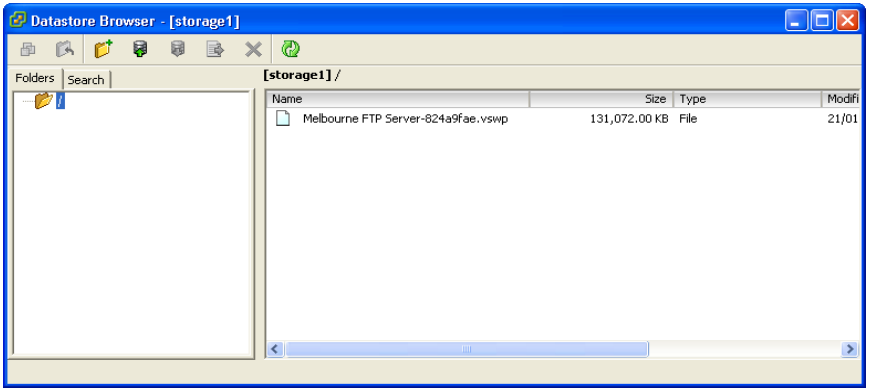


FIGURE E-2 Storage Area

4. From the button bar, click the upload button (database icon with upward-pointing arrow) and upload the IWSVA ISO to this datastore.
5. Close the datastore once the upload is complete.

To create the virtual machine

6. From the menu bar, select **File** > **New** > **Virtual Machine**.

The New Virtual Machine Wizard appears.

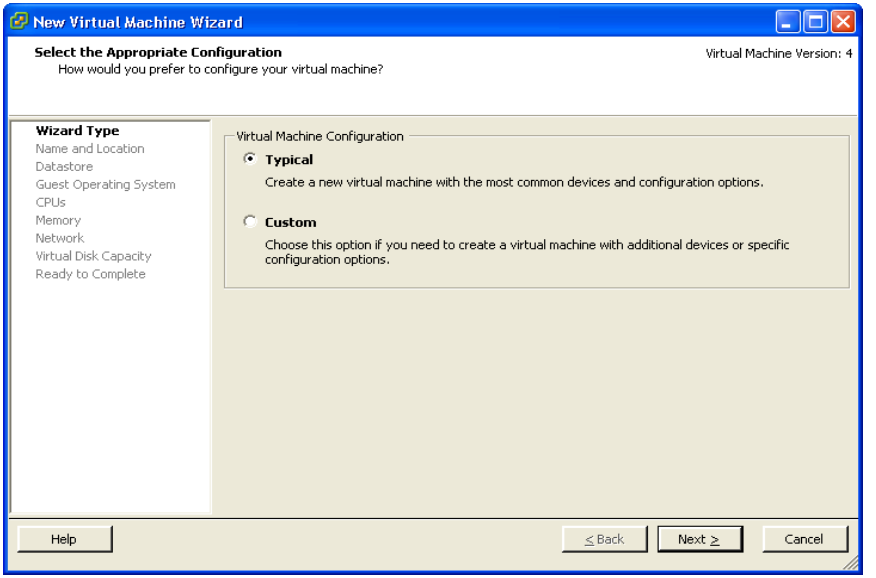


FIGURE E-3 Virtual Machine Configuration

7. Under **Virtual Machine Configuration**, leave the **Typical** button selected.
8. Click **Next**.

The Name and Location Selection page appears.

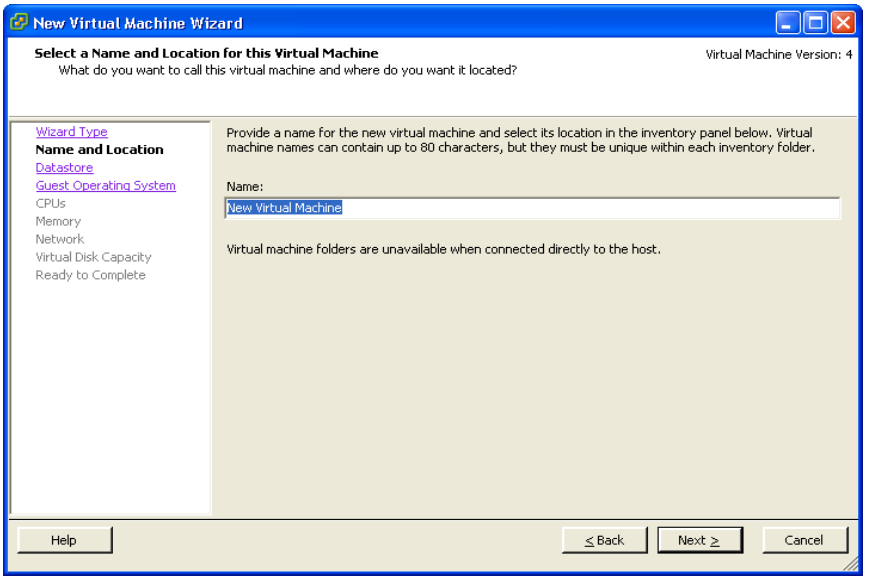


FIGURE E-4 Name and Location of Virtual Machine

9. Type in the **Name** field, an appropriate machine name and then click **Next.**

The Virtual Machine Datastore Selection page appears.

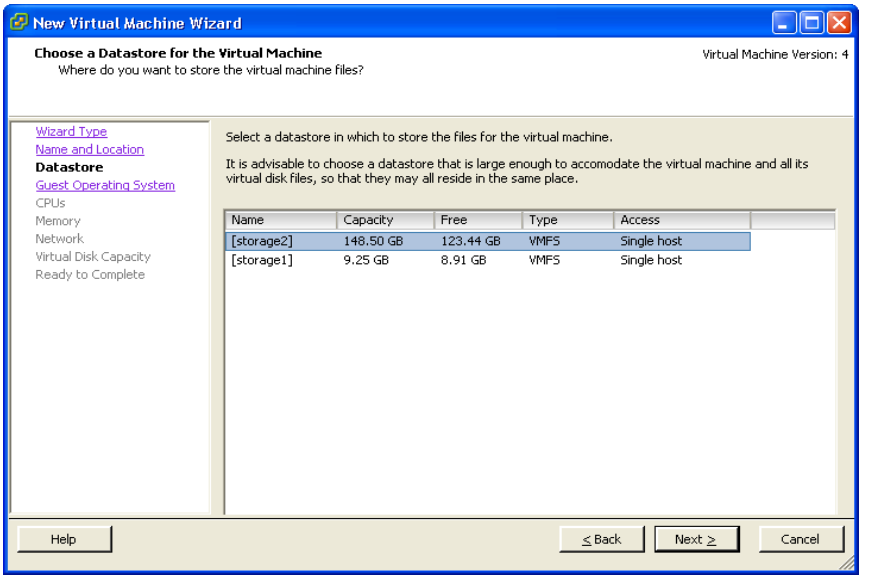


FIGURE E-5 Virtual Machine Datastore

10. Select the datastore where the virtual machine will reside.

This does not have to be the same datastore used to upload the IWSVA ISO.

11. Click **Next**.

The Virtual Machine Guest Operating System screen appears.

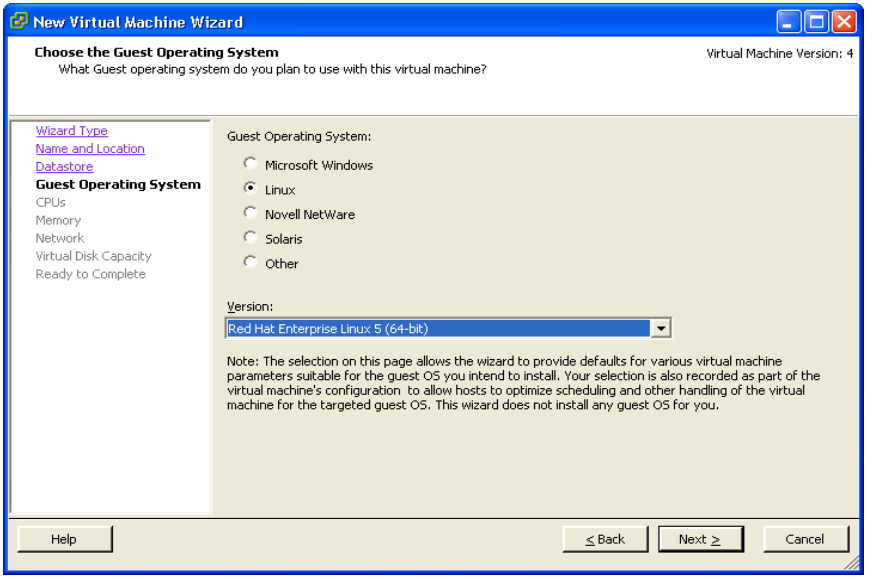


FIGURE E-6 Virtual Machine Guest Operating System

12. For the guest operating system, select Linux and Red Hat Enterprise 5 64Bit.
13. Click **Next**.

The New Virtual Machine Wizard (Virtual CPUs) screen appears.

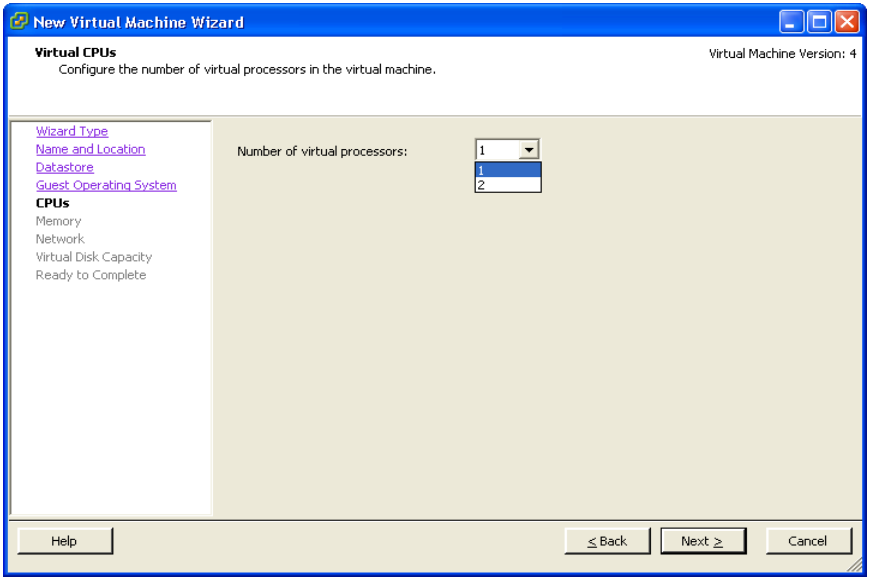


FIGURE E-7 Virtual Machine CPU

14. Select the number of processors for the virtual machine.

IWSVA takes advantage of the Virtual SMP, so select the maximum number of virtual processors available.

15. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears.

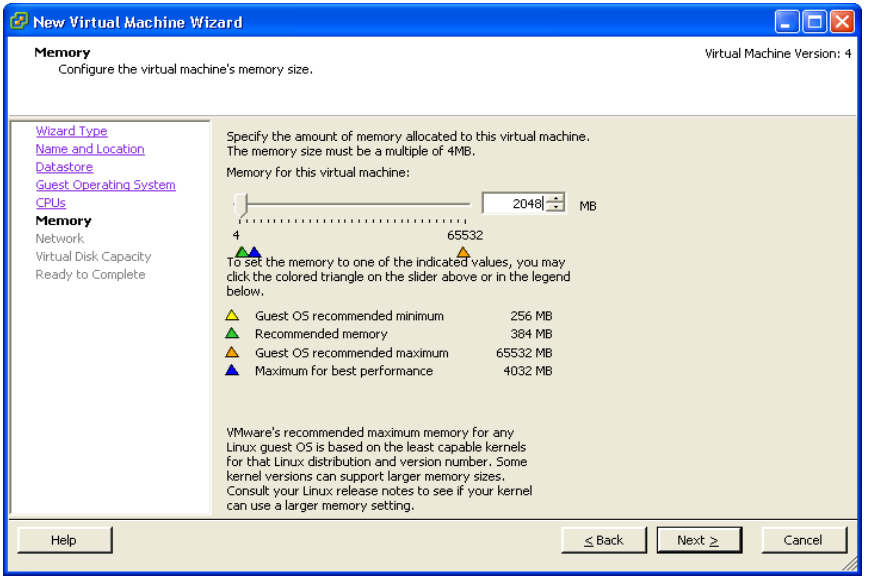


FIGURE E-8 Virtual Machine Memory

16. Allocate 2048 Mb of memory as a minimum for IWSVA.

    For production networks, Trend Micro recommends at least 4096 MB of RAM.

17. Click **Next**.

The New Virtual Machine Wizard (Memory) screen appears.

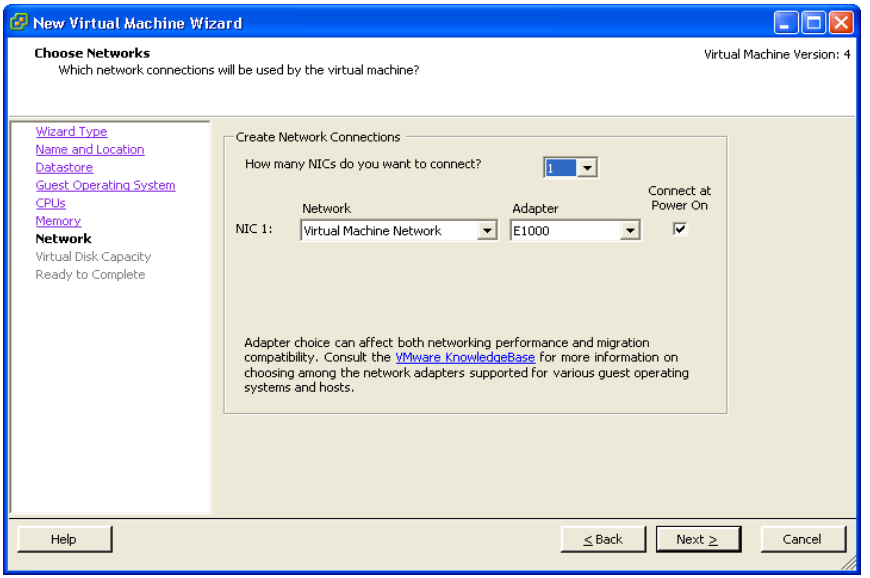


FIGURE E-9 Virtual Machine Network

18. Accept the default network settings and then click **Next**.

The Virtual Disk Capacity screen appears.

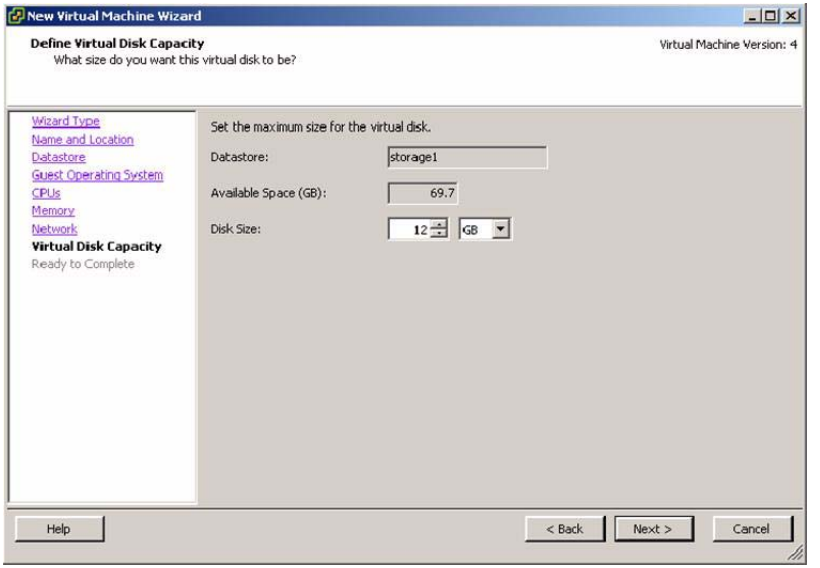


FIGURE E-10 Virtual Disk Capacity

19. For testing purposes, it is adequate to leave the 12GB disk allocation at its default.

For production environments, provide at least 300GB for logging and reporting purposes. See Hardware Requirements on page 1-2 for more information on disk space allocation.

20. Click **Next**.

The New Virtual Machine Wizard (Ready to Complete New Virtual Machine) screen appears.

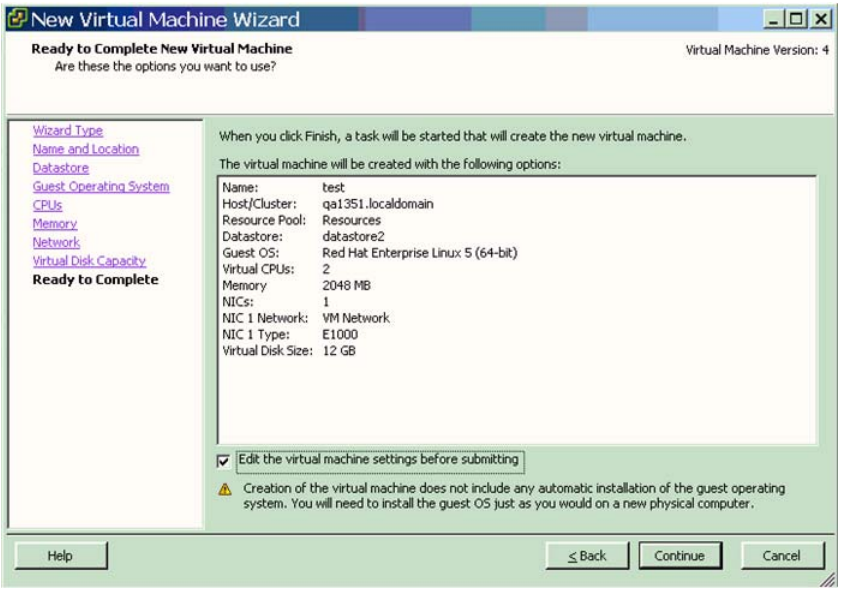


FIGURE E-11 Ready to Complete

21. Check the **Edit the virtual machine settings before submitting** check box and then click **Continue**.

The Virtual Machine Properties screen appears.

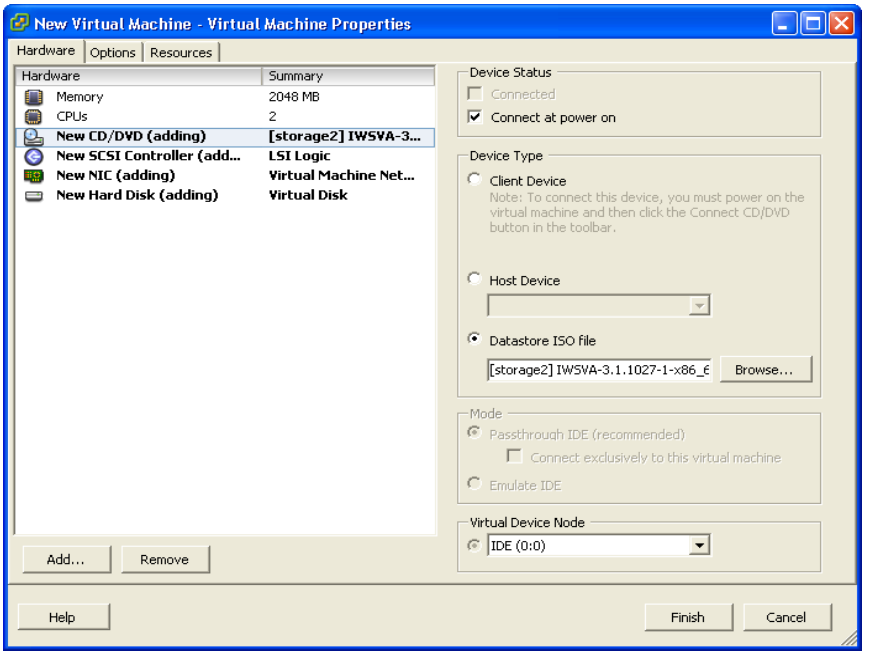


FIGURE E-12 Virtual Machine Properties screen

22. Click on the floppy drive and then click **Remove**.
23. Select the **New CD/DVD** option and then select the **Datastore ISO file** radio button on the right hand side.
24. Click **Browse** and then select the IWSVA ISO that was uploaded in Step 4.

    If you did not copy the Installation ISO onto the VMware server's hard disk, then you can select **Host Device** or **Client Device** from which to load the installer. **Client Device** uses the remote workstation's CD ROM drive to perform the installation and **Host Device** uses the VMware Server's CD ROM drive to perform the installation. Using one of these two methods saves about 500 MB or more of disk space on the VMware server.
25. Ensure that the **Connect at power on** check box for the **New CD/DVD** is checked.

Note: When IWSVA is installed on a VMware ESX server and configured in Transparent Bridge mode, you must enable the virtual switch to accept Promiscuous mode in the ESX 3.5 server.

When deploying IWSVA in bridge mode, do not connect the two data network interfaces to the same switch; otherwise, a loop will be created in your network.

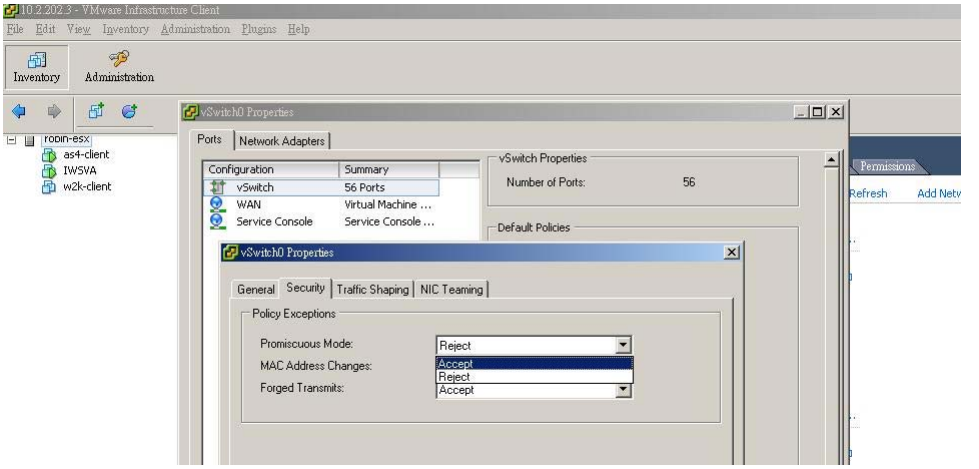


FIGURE E-13 Promiscuous mode in the ESX 3.5 server

26. Click **Finish**.

The new IWSVA 5.0 Virtual Machine is now ready and configured to be powered on and begin the installation process.

Index

A

Activation Code 1-7
Activation Code(s) 3-3
adding policy
  request mode A-25
  response mode A-24
Applet and ActiveX scanning component 3-2
availability requirements A-3

B

Blue Coat Port 80 Security Gateway, setting up A-23
browser requirements 1-3

C

Cisco CE ICAP servers, setting up A-26
Cisco router A-10
client configuration 2-11
client IP to user ID cache B-3
cluster configuration or entry, deleting A-28
components
  installation 3-2
connection requirements A-2
Control Manager
  component 3-2
Control Manager, TMCM, Trend Micro Control Manager 1-6

D

Damage Cleanup Services
  non-HTTP malware A-8
Damage Cleanup Services (DCS) A-7, A-9
  using HTTPS A-9
database 1-6
  troubleshooting B-6
database requirements 1-4
database type and location 1-6
DCS A-7
DCS, A-9
Demilitarized Zone 2-2
Dependent mode
  FTP proxy 2-9
dependent mode
  double proxy 2-20
  HTTP double proxy 2-21
  HTTP proxy ahead 2-17
  HTTP proxy behind 2-19
  HTTP reverse proxy 2-30
directory (LDAP) server
  performance B-2
  requirements 1-4
directory servers 1-4
distributed environment A-2
DMZ 2-2

E

EICAR C-1
EICAR test file C-1, D-7
enable_ip_user_cache B-3

F

FTP
  flows 2-7
  scanning component 3-2
  services 2-4
  upstream proxy 2-8
FTP over HTTP 2-12

G

Global Catalog A-5
glossary D-7

H

hardware requirements 1-2
HTTP
  scanning component 3-2
  services 2-4
HTTP and FTP service flows 2-5
HTTP/FTP
  server protection A-19

I

ICAP 2-23
  compliant cache server, setting up A-20
  for Blue Coat appliances A-23
  for Cisco CE servers A-26
  for NetCache appliances A-21
  license key A-21
  requirements 1-4

ICAP installation notes A-20
ICAP mode
  HTTP proxy 2-25
  multiple servers 2-27
Installation
  Blue Coat Port 80 Security Appliance, A-26
installation 1-1, 3-1–3-2, 4-1
  Blue Coat Port 80 Security Appliance, A-23
  existing FTP proxy 2-8
  necessary information 1-5
  NetCache Appliance A-21
Intellitunnel Security component 3-2
Internet Content Adaptation Protocol 2-23
ip_user_central_cache_interval B-3
IWSVA
  components 3-2
  testing C-1
IWSVA ICAP
  multiple server services A-22
IWSVA server
  placement with one firewall, no DMZ 2-3
  placement with two firewalls in DMZ 2-2

J

Java Runtime A-24

K

Knowledge Base 1-xii, D-5
  URL 1-xii, D-4
known issues D-5
  Knowledge Base D-6
  readme D-5

L

Layer 4 switch 2-13
Layer 4 switches 2-12
LDAP
  integration A-4
  requirements 1-4
License Agreement D-2

M

main program 3-2
maintenance D-2
Maintenance Agreement D-2
  defined D-2
  expiration D-2
  renewal D-2–D-3
  renewing D-3
Microsoft SQL Server Desktop Engine (MSDE) 1-6
multiple servers 2-27

N

NetCache Appliance, setting up A-21
network traffic 1-7

O

online help 1-xii
operating system
  requirements 1-2

P

patches D-2
performance tuning B-2
phish C-11
post installation 3-24
product maintenance D-2
product updates D-2
proxy
  configuration 1-6
  updates 1-7

R

readme 1-xi, D-2
referral chasing A-4
registration
  URL D-3
Registration Keys 1-7
Registration Profile D-3
removing 1-1, 3-1, 4-1
requirements 1-2
risk ratings D-7

S

Security Information Center D-7
SNMP 1-6
SNMP notification component 3-2
SolutionBank-see Knowledge Base 1-xii
SSL
  DCS A-9
standalone mode 2-15
  FTP proxy 2-7

HTTP proxy 2-15
multiple servers 2-16
suspicious files D-6

T

technical support D-4
URL D-4
testing
download scanning C-8
FTP scanning C-5
PhishTrap C-11
spyware scanning C-10
upload scanning C-2
URL filtering C-7, C-9
throughput requirements A-3
TMCM
component 3-2
Trend Micro
contact information D-4
Trend Micro Control Manager
component 3-2
TrendLabs D-4, D-8
troubleshooting D-8

U

Update Center D-2
URL filtering component 3-2
URLs
Knowledge Base 1-xii, D-5–D-6
readme documents D-5
registration D-3
Security Information Center D-7
technical support D-4
user authentication cache B-3
user group membership cache B-3
user_groups_central_cache_interval B-3

V

verbose logging B-4
virus
scanning server clusters, configuring A-27
virus alert service D-8
virus doctors-see TrendLabs D-5
Virus Encyclopedia D-7
Virus Map D-7
Virus Primer D-7
virus scanning server clusters
server clusters A-27
Visual Policy Manager A-24

W

Web console password 1-6
weekly virus report D-7
white papers D-8

X

X-Infection-Found A-28
X-Virus-ID A-28